

**John Gibb**

**CINE TE URMĂREȘTE?**

JOHN GIBB

TOP SECRET

CINE

te urmărește?

adevărul  
înpăimântător  
despre Stat,  
supraveghere  
libertate personală



*rao international publishing company*

Descrierea CIP a Bibliotecii Naționale a României

JOHN GIBB

Cine te urmărește? / John Gibb; trad.: Ionuț Mihai Fulger.  
— București: RAO International Publishing Company, 2009

ISBN 978 – 973 – 54 – 0069 – 9

I. Fulger, Ionuț Mihai (trad.)

821.111 – 31 = 135.1

RAO International Publishing Company

Grupul Editorial RAO

Str. Turda nr. 117 – 119, București, România

[www.raobooks.com](http://www.raobooks.com)

[www.rao.ro](http://www.rao.ro)

JOHN GIBB

*Who if watching you?*

Copyright © Conspiracy Books 2005

Toate drepturile rezervate

Traducere din limba engleză

Ionuț Mihai Fulger

© RAO International Publishing Company, 2006

pentru versiunea în limba română

mai 2009

ISBN 978 – 973 – 54 – 0069 – 9

## Prefață

Pe 11 septembrie 2001, la 8.45 a.m., lumea s-a schimbat – brusc și definitiv. Acesta a fost momentul în care zborul 11 al American Airlines a intrat în Turnul dinspre nord al World Trade Center din New York. După 18 minute, zborul 175 al United Airlines a lovit turnul dinspre sud. Acesta din urmă s-a prăbușit primul, la 9.58 a.m. Turnul dinspre nord s-a năruit și el după o jumătate de oră. Pentru Statele Unite ale Americii, aceasta a reprezentat o atrocitate înfiorătoare declanșată – aparent fără avertizare – de către Al Qaeda, pe atunci doar o organizație teroristă islamică obscură și subestimată, care opera din peșterile adânci ale munților din Afghanistan. Șocate și silite să reacționeze, Statele Unite au ripostat, folosindu-și întreaga forță militară, pentru a distruge guvernul taliban al Afghanistanului, care îi adăpostise pe făptași, și de a scoate Al Qaeda din fortărețele ei subterane.

Însă, pe lângă acest conflict foarte sângeros, Statele Unite au pornit un război secret împotriva unui dușman invizibil: rețeaua teroristă mondială, alcătuită din membrii și susținătorii Al Qaeda. Atacul din 9/11 fusese plănuțit cu meticulozitate. Cei 19 bărbați care l-au executat erau bine antrenați, finanțați cu dărnice și aveau inestimabilul avantaj de a fi dispuși să moară pentru cauza lor. Această combinație de bani, inteligență și hotărâre punea guvernul american într-un pericol fără precedent, căruia trebuia să îi corespundă o replică intransigentă – cel puțin în ceea ce privește libertățile cetățenești. Statele Unite au răspuns prin înființarea rapidă a Departamentului Securității Interne, precum și prin elaborarea și intrarea în vigoare a legii „Patriot Act”, decizii care – combinate cu spaima provocată de atacul propriu-zis – au declanșat paranoia și confuzie în rândul polițiilor și agențiilor de securitate.

Deodată, aceste măsuri au subminat grav multe dintre drepturile și libertățile care fuseseră păstrate cu sfințenie în

Constituția Statelor Unite și apoi întărite prin nenumărate sentințe juridice. Administrația Statelor Unite a investit sume uriașe în dezvoltarea unor sisteme prin care să poată ține sub observație publicul și schița un profil comportamental pentru orice persoană care ar fi putut fi bănuită că este un „inamic al statului”. Toate acestea au dat naștere unui climat de teamă, în care supravegherea cetățenilor americani a putut fi sporită, devenind astfel chiar și mai intensă, dar pe deplin justificabilă pentru un popor american care nu se dezmeticise încă după șocul provocat de atacul Al Qaeda.

Noi, britanicii, am urmărit furtuna izbucnită în Statele Unite și ne-am reamintit că trecuserăm și noi prin toate astea, când cu Armata Republicană Irlandeză (IRA). Însă, fără îndoială, în comparație cu ambițiile globale ale Al Qaeda, Irlanda de Nord nu depășea cu mult proporțiile unei mici încurcături provinciale. În numai câteva luni, am arestat grupuri de extremiști islamici care, din câte se părea, se aflau în Marea Britanie ca să ne ucidă pe toți în propriile paturi. În 2005, guvernul britanic, în frunte cu premierul Tony Blair, a încercat să transforme amenințarea reprezentată de teroriști, precum asasinul condamnat Kamel Bourgass, într-o justificare suficientă pentru a introduce noi restricții, fără precedent, ale libertăților cetățenești: detenție pe termen nedefinit fără să existe nicio acuzație, folosirea injustiție a mărturiilor obținute sub tortură (chiar dacă în afara țării), mandate de arestare emise mai degrabă de politicieni decât de judecători și restricții ale accesului în clădiri publice, incluzând – chiar și Parlamentul.

Așadar, ce se petrece? Lumea liberă este cu adevărat amenințată sau totul face parte dintr-o conspirație menită să ne erodeze prețioasa intimitate și libertățile personale? Această carte schițează câteva întrebări și oferă câteva răspunsuri. Faptul că suntem cu toții urmăriți nu poate fi negat. Însă cât de atent? Și de către cine?

## Introducere

*E dificil de apreciat impactul unui atac terorist dacă tu însuși nu ai cunoscut direct unul. În cazul meu, a fost un amestec de farsă și stinghereală. Singurul element serios a fost faptul că era primul dintr-o lungă serie de atacuri ale republicanilor irlandezi asupra Marii Britanii. Ne-am trezit deodată atacați cu bombe făcute din îngrășământ agricol, îndesate în mașini de către niște puști din clasa de mijloc (incompetenți, însă decizi), unii dintre ei vărsându-și mânia generată de o moștenire de opresiune și resentimente cu rădăcinile în Evul Mediu.*

8 martie 1973. Ziua a început cu triluri de păsări și un soare plăcut de primăvară. Apoi, după prânz, o adiere de vânt rece a început să șfichiuiască dinspre vest, unduind suprafața Tamisei și desenând o pătură de nori cenușii, plutind la înălțime mică deasupra orașului. Mergeam pe Whitehall Place, îndreptându-mă spre Ministerul Agriculturii. Muncitorii Consiliului Local al Londrei își încărcau camionul, după ce curățaseră ferestrele Clubului Național Liberal, aflat pe partea vestică a străzii. Orologiul Big Ben bătea de trei fără un sfert, în timp ce eu mă îndreptam spre Whitehall. Mi-au mai trebuit cinci minute pentru a urca scările din dreptul intrării în minister și am zăbovit câteva clipe, privind arcada de piatră albă, cu reliefurile ei sculptate, care întruchipa scoici și snopi de porumb – opera unor deținuți, mi s-a spus cândva, ai închisorii Verne de pe insula Portland.

În jurul orei trei fără zece, a explodat bomba. Una puternică, făcută din vreo 80 de kilograme de îngrășământ agricol, după cum s-a dovedit ulterior. Se afla într-un pachet plasat sub scaunele unui Hillman Hunter de culoarea bronzului, parcat chiar în spatele clădirii. Mașina fusese furată în Belfast și adusă la Dublin în urmă cu trei săptămâni. I se

schimbaseră plăcuțele de înmatriculare și apoi fusese transportată cu feribotul de la Dun Laoghaire la Fishguard și apoi la Londra. Dis-de-dimineață, Dolours, fiica unui vechi membru al Armatei Republicane Irlandeze (IRA), Albert Price, un fanatic și nemilos „provo” (membru al facțiunii paramilitare IRA), condusese Hillmanul din Dolphin Square la Biroul de Recrutare din Great Scotland Yard, și îl lăsase acolo. La trei fără șase minute, dispozitivul a fost detonat cu una dintre amorsele de fabricație cehoslovacă dintr-un transport de marfă donat de colonelul Ghaddafi, liderul libian, și adus clandestin în țară. În total, în acea zi patru mașini-capcană fuseseră abandonate în centrul Londrei de către membri ai IRA. La ora unu, presa primise telefoane de avertisment, în care erau divulgate numerele de înmatriculare și pozițiile mașinilor-capcană. Poliția metropolitană, pe vremea aceea deloc iute ca fulgerul, a reușit să găsească două dintre bombe, iar ofițeri din echipa pirotehnică de intervenție le-au dezamorsat. Eu am fost victima celei de-a treia bombe. A patra a explodat după șase minute, în față la Old Bailey. Am auzit eoul unei bufnituri metalice în timp ce zăceam la pământ, holbându-mă la o băltoacă de sânge care se formase în dreapta mea.

Energia exploziei din Great Scotland Yard a fost limitată de un bloc compact de grajduri vechi către nord-est și comprimată de vehiculele parcate în față și în spate. Suflul și-a găsit o cale de scăpare pe Whitehall Place, unde a erupt, bubuind ca o furtună sub arcada de deasupra Scotland Place și aducând cu sine cioburi de sticlă și bucăți de metal. Mi s-a spus apoi că vidul provocat de explozie spărsese toate geamurile din Whitehall Place și că eu fusesem prins de extremitatea sa. După câteva secunde, când am reușit să-mi revin în simțiri, m-am trezit așezat pe la jumătatea scărilor, cu un ciob de sticlă înfipt în mine și cu părul plin de praf și geam pisat. Nu am știut exact ce se întâmplase decât mult mai târziu în acea zi, când am aflat din *London Evening News* că fusesem lovit de prima bombă a campaniei continentale purtate de IRA. Bomba de la Old Bailey, plantată într-un Ford

Cortina verde, a rănit 186 de persoane. Un bărbat a murit ulterior, ca urmare a unui atac de cord care, a susținut poliția, fusese provocat de trauma detonării. Cei răspunzători pentru atac au fost arestați de poliție și acuzați de crimă.

Am stat o vreme pe trepte, privindu-i pe polițiști venind în fugă din Charing Cross și grăbindu-se de-a lungul străzii, oprindu-se doar pentru a sparge cu bastoanele geamurile mașinilor parcate și urlând unul la altul, cu voci ascuțite, pline de panică și adrenalină. Cineva le ordonase să se răspândească și să caute obiecte suspecte în mașini. Ofițerii din echipa pirotehnică stăteau împrejur – fie în picioare, fie așezați în mașinile lor Land Rover – și fumau, în așteptarea unor instrucțiuni. Mi se părea că zăcusem pe trepte mult timp, deși știu că nu putuseră fi mai mult de câteva minute, și începea să-mi fie clar că Whitehall se golise. Oamenii fugiseră sau fuseseră evacuați din Parlament și clădirile guvernamentale. Whitehall, Victoria Street, Embankment și podul Westminster erau deodată pustii și tăcute, cu excepția ecourilor alarmelor de pe mașinile poliției, care accelerau către capătul străzii. Se pare că trăiam un sentiment de detașare de totul din jur, atunci când un polițist în uniformă, cu o privire sălbatică, a traversat strada către mine, țișând incoerent. S-a postat alături și mi-a ordonat să mă ridic, astfel încât să mă poată percheziționa. Sergentul său a alergat în sus pe scări, pentru a-l domoli înainte să mă ridice și să mă conducă în clădirea ministerială.

Picioarele îmi tremurau și mă simțeam de parcă fusesem lovit într-o parte de un boxer profesionist. Holul de la intrare, cu marmură și mahon, era plin de freamăt, dar nu m-a întâmpinat nimeni, așa că am luat o ceașcă cu ceai și l-am rugat pe sergentul de poliție care făcea de gardă să-i transmită portarului că venisem la întâlnirea, fixată pentru ora trei, cu ministrul Jim Prior, în acel moment, eu păream singura victimă a atacului. Însă aveam să descopăr în curând că mă înșelam. Când, în cele din urmă, personalul de securitate m-a dus afară, unde aștepta o mașină ministerială, ei și-au cerut scuze pentru penuria de ambulanțe, deoarece toate vehiculele



de intervenție disponibile fuseseră trimise pentru a se ocupa de răniții de la Central Criminal Court (Tribunalul Penal Central). I-am cerut șoferului să mă ducă înapoi la *Sunday Express*, unde lucram pe atunci. Fără să-și ia ochii de la drum, el îmi spuse: „Nu face pe nebunul, băiete. Te duc la spital”.

Eră ora patru când am depășit în viteză piața Horse Guards Parade. Regimentul de cavalerie își înlocuise deja gardienii călare cu soldați severi, purtând armură de corp și ținând în mâini arme de asalt. Exista un sentiment de irealitate, ca și cum lumea noastră familiară se sfârșise și nimic nu avea să mai fie la fel. Am aflat mai apoi, ascultând ce se vorbea în secția de urgență a spitalului Middlesex, că zece bărbați și femei de origine irlandeză fuseseră arestați la aeroportul Heathrow. Marea Britanie fusese „închisă” și transformată într-un câmp de luptă, nu mai avea nimic din terenul de joacă pe care îl știam. În acea zi se împlineau fix 25 de ani de când George Orwell înmânase editorilor săi manuscrisul romanului *1984*.

Douăzeci de ani mai târziu, pe 24 aprilie 1993, IRA a adus o camionetă plină cu explozivi în City (zona cunoscută și ca „Square Mile”) și l-a detonat în Bishopsgate, avariind grav Natwest Tower de pe Old Broad Street, numărul 25, și închizându-l. Acest colos ostentativ fusese proiectat de Richard Seiffert și finalizat în 1980, după ce fuseseră investite în el 72 de milioane de lire sterline. Din fericire pentru cei care lucrau acolo, clădirea era solidă, cu un miez din beton care susținea cele 42 de etaje. Nimeni nu a fost ucis, însă violența și îndrăzneala atacului au avut un efect profund asupra lumii corporatiste din City. Rezultatul a fost un efort susținut al instituțiilor financiare din zonă de a-i proteja pe bogați de nebuni, investind în cel mai înalt nivel de securitate posibil. Revolta bărbaților în costume a fost sprijinită de buzunarele lor încăpătoare, iar răspunsul poliției și al forțelor de securitate a venit imediat. Dacă să-i bombardezi pe politicieni și pe clienții puburilor părea acceptabil, un atac în City era cu totul altceva. Nu putea exista niciun fel de toleranță față de teroriștii care periclitează piețele financiare

și de asigurări, ca să nu mai vorbim de integritatea clădirii Old Bailey, leagănul justiției și cel mai mare tribunal din lumea occidentală.

La câteva zile după atacul de la Natwest, un cerc de beton și oțel fusese înălțat în jurul zonei Square Mile, iar polițiști în uniformă opreau și verificau fiecare mașină ce intra în City. În același timp, camere de supraveghere au început să răsară pe monoliticele clădiri de birouri, ca niște mici protuberanțe fixate pe pereți, la șapte metri înălțime. Unele se mișcau odată cu tine, altele arătau, prin aprinderea unui buton roșu, că înregistrează. O unitate de monitorizare a fost înființată și echipată pe Wood Street, fiind sub controlul secției de poliție Bishopsgate. În mai puțin de un an, poliția din City dădea ordin ca sisteme de televiziune cu circuit închis să supravegheze până la ultimul centimetru din străzile și trotuarele din Square Mile. Nu mai exista nicio curte, niciun garaj sau scuar care să nu poată fi monitorizat sau înregistrat, iar polițiștii nici măcar nu aveau nevoie să apeleze la Ministerul de Finanțe pentru fondurile necesare. Supravegherea era plătită independent de bănci și instituții financiare, iar sistemul era proiectat după cerințele acestora. Banii nu constituiau o problemă.

Pe la începuturile actelor de violență ale IRA, serviciile de securitate din afara Londrei dădeau un răspuns neașteptat de firav forțelor teroriste, bine finanțate. Informațiile erau puține, iar în scurt timp, grupul de „provo” a devenit imprevizibil și fără scrupule. În primele zile ale sistemului de supraveghere din City, calitatea videocamerelor și a casetelor era standard, iar imaginile erau în alb-negru. Nu exista facilitatea de a mări un detaliu sau de a lărgi perspectiva, după cum nu existau nici sunet, nici posibilitatea de a identifica un număr de mașină, nici capacitatea de a recunoaște și de a capta trăsăturile faciale ale trecătorilor, nicio arhivă digitală. Erau acoperite parțial activitățile din stațiile de metrou, iar cei care priveau ecranele nu erau foarte pricepuți la asta. Vizitatorilor centrului de supraveghere îi se ofereau proiecții din videotecă, ce includeau exhibiționiști

care, ca urmare a vreunui pariu, se apucaseră să alerge goi între puburile The Green Man din Victoria Street și Bishop's Finger din Smithfield. Ofițerii de poliție cărora li se dăduse sarcina de a sta în fața unui șir de ecrane de televizor, așteptând să se întâmple ceva, au găsit treaba asta dificilă și plictisitoare, așa că, după cum era de așteptat, au folosit echipamentul video pentru a înregistra evenimentele care spărgeau monotonia. Totuși, instituțiile s-au dedicat securității cu hotărâre și fără compromisuri. Consilierii municipali și-au scos carnetele de cecuri, polițiștii au fost puși la punct, iar bancherii și asigurătorii au putut dormi liniștiți, acordând din nou afacerilor întreaga lor atenție.

Corporația s-a lăudat că fiecare centimetru din Square Mile putea fi supravegheat de poliție. Orice îngrijorare publică pe care această declarație ar fi putut-o provoca nu a fost luată în considerație până când această supraveghere nu a devenit un *fait accompli*. Atunci când organizațiile de apărare a libertăților cetățenești s-au trezit, în sfârșit, începând să pună întrebări și să dea glas neliniștilor lor, acestea au fost respinse violent de adjunctul șefului poliției din City și ministrul de interne. Când vine vorba de războiul antitero, nimănui nu-i mai pasă de sensibilitățile publicului. Vechile alei dimprejurul Băncii Angliei, „Bătrâna doamnă din Threadneedle Street”, erau acum curățate. Prostituatele din Cheapside și Barbican au ales fie să renunțe la meserie, fie să se mute în Tower Hamlets, Southwark sau West End. În timp ce fraudele și infracțiunile financiare au rămas la fel de obișnuite ca și înainte, jafurile armate, furturile și actele de violență stradală au devenit amintiri în City. Atunci când atrocitățile comise de IRA au continuat în provincie și în West End, și mai multe resurse au fost folosite pentru a proteja inima de aur a Capitalei, iar supraveghetorii au fost instruiți să îmbunătățească performanțele sistemelor lor cu ajutorul unui program care recunoștea și atenționa poliția asupra prezenței unei mașini furate în nici trei secunde de la intrarea ei în City.

Sistemul de supraveghere din City, cu programul său de identificare automată a numerelor de mașină, s-a dovedit o

pedică de succes în calea atacurilor cu mașini-capcană și urmează să fie extins în întreaga Mare Britanie, într-o primă fază în 23 de unități de poliție din Anglia. Teoretic, sistemul va fi utilizat pentru a da de urma celor opt milioane și jumătate de mașini care fie nu sunt cu taxele la zi, fie nu sunt asigurate, fie sunt suspectate de conexiuni cu activități infracționale sau cu terorismul. Camerele de supraveghere, acum capabile de a monitoriza 3.500 de autovehicule pe oră, vor fi instalate în puncte fixe și montate în dube ale poliției. Ele caută nu atât șoferi proști, cât infractori motorizați. Totuși, există o varietate de sisteme active, inclusiv unul constând dintr-o serie consecutivă de camere ascunse, care cronometrează un autovehicul de-a lungul unui kilometru și jumătate de șosea. Sistemul este astfel conceput încât să se ocupe de mașinile cu viteză care încetinesc atunci când șoferii știu că se apropie o cameră de înregistrare, pentru că prin el se poate calcula viteza medie a autovehiculului pe parcursul întregului traseu. Autorităților le place acest sistem, deoarece el nu face nicio discriminare. Programul nu se întreabă dacă vinovăția șoferului în chestiune merită pusă la îndoială sau nu, el nu poate judeca subiectiv, precum un ofițer de poliție în uniformă. Nu există decât două opțiuni: încălci legea sau nu.

Sistemele de supraveghere și tehnologiile se îmbunătățesc permanent; deja nu mai există nimic care să oprească poliția și serviciile de securitate să conecteze sistemul la baza de date a Autorității pentru Șoferi și Autovehicule (DVLA) din Swansea (Țara Galilor), în care se regăsesc numele și adresa fiecărui posesor de mașină din țară. Aceasta le va permite polițiștilor nu numai să tragă pe dreapta automobilisti, pentru tichete de parcare neplătite sau amenzi datorate depășirii vitezei regulamentare, ci și să urmărească traseele lor zilnice. Pericolul în ceea ce privește libertățile cetățenești este că astfel li se oferă posibilitatea agențiilor de păstrare a ordinii publice – și, ca atare, statului – de a-și construi o imagine cuprinzătoare asupra deplasărilor și comportamentului nostru, precum și de a trage concluzii despre noi, pe baza datelor înregistrate. Această analiză nu este realizată de un comitet

sau de un funcționar așezat la un birou, ci de un computer, care a fost programat să ajungă la niște concluzii pornind de la date provenind din diferite surse. Un exemplu este sistemul Carnivore, utilizat de FBI, care înregistrează obiceiurile de lectură ale unei persoane, pe baza fișelor de bibliotecă și a achizițiilor de cărți. Odată ce se știe ceea ce citim, nu mai e decât un mic pas până la formarea unei opinii asupra încrederii și adevărului noastre politice. Iar aici libertatea se sfârșește.

Supravegherea de rutină a mulțimii, prin utilizarea unei televiziuni cu circuit închis (CCTV), devine chiar și mai îngrijorătoare atunci când este combinată cu alte invenții recente. Acum, Ministerul de Interne și serviciile de securitate ascultă în mod curent convorbirile telefonice, fără a mai avea nevoie de vreun mandat acordat de un judecător. De asemenea, se experimentează programe concepute pentru a identifica fețele oamenilor, pe baza unei arhive de poze, ale căror surse sunt rapoartele de arestare, Biroul Pașapoarte și alte agenții guvernamentale ce solicită identificarea fotografică. Tehnologia este deja utilizată de industria jocurilor de noroc din Statele Unite și este în curs de introducere, în taină, într-unul sau două cazinouri din Londra. Această industrie practică frecvent schimbul de informații despre jucătorii suspecți că ar trișa. Jocul 21 sau ruleta sunt în mod special vulnerabile în special când sunt profesioniști în joc, așa că participanții sunt urmăriți și înregistrați permanent. Jucătorii nedorți, aflați pretutindeni pe lista neagră, sunt filmați pe ascuns și identificați imediat ce intră în clădire, iar apoi le este refuzat accesul în sala de jocuri. Panica generată în rândul personalului de securitate de căderea unui sistem de supraveghere este groaznic de urmărit. Totuși, acuratețea recunoașterii faciale este discutabilă, spre deosebire de testul ADN sau de înregistrarea irisului.

De la începuturile campaniei IRA din anii 1970, apoi după apariția în Europa a unor varii grupări teroriste locale (ca Brigăzile Roșii în Italia sau Facțiunea Armata Roșie în Germania), măsurile de protecție a intimității și a datelor

personale au fost lăsate deoparte, în mod frecvent, în momentele de alertă națională. Fiecare regulă încălcată tinde să rămână așa mult timp după ce amenințarea aparentă a fost înlăturată sau s-a dovedit a fi inexistentă. De pildă, istoria detenției suspectilor de terorism în închisoarea Long Kesh din Irlanda de Nord, în anii 1970, a făcut ca ministrului de interne să-i fie mai ușor, trei decenii mai târziu, să-i întemnițeze pe extremiștii islamici în închisoarea Belmarsh și să-i țină acolo fără să le fie intentat proces. Informațiile strânse pentru propusa bază de date a cărților de identitate vor fi disponibile și pentru alte agenții guvernamentale, precum Administrația Financiară sau Departamentul Vamă și Accize. Pe măsură ce perceputa amenințare teroristă crește, presiunea exercitată asupra literei legii de către politicieni devine tot mai puternică. Am asistat deja la intense presiuni de a desființa sistemul cu jurați și prezumția de nevinovăție pentru multe infracțiuni, atât aici, cât și în Statele Unite. Cât va mai dura oare până când un ministru britanic de interne se va împotrivi dorințelor serviciilor de securitate și va cere includerea convorbirilor telefonice înregistrate printre dovezile acceptabile în justiție?

Principala justificare oferită pentru toate aceste atacuri asupra libertăților individuale este amenințarea terorismului, care astăzi, după 9/11, poate scuza orice măsură extremă. Atunci când guvernul exagerează sau minte în ceea ce privește această amenințare, pătrundem într-o epocă periculoasă a istoriei.

În tinerețea mea, când Churchill era prim-ministru, ideea că el ar minți poporul pentru a intra în război era de neconceput. O fi fost el un bătrân ticălos, dar niciodată nu existase vreo îndoială că ținea la interesele națiunii. Churchill era un luptător și un soldat. Fusesse educat să-și servească țara și stătuse în captivitate, ca prizonier de război, în Africa de Sud. Astăzi în schimb, deși încă nu prea pare să ne pese, suntem conduși de politicieni pentru care interesele de partid și dorința personală de putere sunt mai presus de orice.

Introducerea noilor cărți de identitate în Marea Britanie

este mult mai importantă decât ni se pare. Prin această măsură, deplasările și activitățile fiecărui cetățean pot fi înregistrate și arhivate în baze de date pentru securitate, care vor fi operate de companii private de securitate. Pe măsură ce tehnologia evoluează, va veni o vreme – mai devreme decât ne așteptăm – în care un fișier electronic conținând datele noastre de sănătate, limita de creditare bancară, călătoriile în străinătate, voturile la alegeri, alături de fiecare mișcare sau decizie pentru care trebuie să prezentăm un act de identitate, va fi disponibil unui funcționar civil și, deci, unui politician, care s-ar putea să nu aibă la inimă interesele noastre. Este greu de înțeles ce avantaje va oferi cetățenilor un asemenea sistem. În cazul unei amenințări teroriste autentice, este ridicol să ne imaginăm că un sinucigaș cu bombă foarte hotărât va fi împiedicat de necesitatea de a deține o bucatică de plastic. Politicienii ne spun că aceste cărți de identitate ne vor ajuta să ne protejăm granițele de cei nepoftiți, dar se pare că nimeni nu s-a gândit la problema graniței libere dintre Republica Irlanda și Marea Britanie. Pe de altă parte, cunoașterea este putere, nu-i așa? Iar politicienii de azi vor găsi o cale de a ieși din această dilemă. Baza de date cu cărți de identitate, împreună cu toate bazele de date asociate ale agențiilor guvernamentale, va da statului o putere fără precedent de a-și băga nasul în viețile noastre private.

De la distrugerea World Trade Center, spaima de terorism a devenit o parte a dietei noastre politice zilnice, un adevărat *raison d'être* pentru nenumărate exemple de exces politic. Oamenii din umbră, experții în tehnologie și stăpânii lor politici au acum un cuvânt greu de spus în viețile noastre, atât aici, cât și în SUA. Supraveghetorilor le stă în fire să strângă și să arhiveze tot ce pot afla despre noi, iar apoi să țină secrete datele deținute. Despre asta vorbește această carte.

# Capitolul I

## Tu cumperi, noi veghem

*Cu mulți ani în urmă, viața cotidiană era o chestiune mai degrabă simplă. Lumea mergea la muncă, se ducea în oraș să cumpere fructe și legume de la piață, pâine de la brutărie și carne de la măcelărie. Era cu totul de neconceput ideea că, într-o zi, ai putea fi filmat în timp ce te duci la muncă, fotografiat în timp ce conduci mașina, monitorizat în timp ce îți alegi și plătești cumpărăturile, că ar putea exista carduri de loialitate care să te individualizeze și baze de date care să fie actualizate când îți plătești facturile. Dar iată că toate acestea s-au întâmplat oricum. Practic, tot ceea ce facem este înregistrat și stocat undeva. Iar nouă nu s-ar zice că ne pasă prea mult. Probabil, pentru că nu ne dăm seama în ce măsură renunțăm, zi după zi, la propria intimitate. La urma urmei, n-am greșit nimănui cu nimic, așa că nu avem de ce să ne temem. Așa să fie oare?*

În cursul ultimilor 30 de ani, supravegherea informatizată a centrelor orașelor, ca măsură de luptă împotriva terorismului, a crescut constant și aproape fără nicio restricție, cu efecte dramatice asupra vieții urbane din Marea Britanie. Nimeni nu pare a ști cu exactitate câte camere de supraveghere ne urmăresc, însă chiar și cele mai optimiste estimări sunt de ordinul milioanei. Clive Norris, profesor de criminologie la Universitatea din Hull, a publicat recent propria analiză pe marginea acestui subiect. Numărul camerelor de filmat active în spațiul public din Marea Britanie a fost estimat de el la trei milioane. „Este dificil să furnizezi o cifră exactă. Nu toate sistemele de supraveghere se încadrează în Legea protecției datelor, dar credem că o aproximare moderată ar fi între două



și trei milioane de unități de înregistrare individuale. Altfel spus, cam două camere la 30 de oameni”, susține Simon Davies, director al organizației de apărare a drepturilor omului Privacy International. Se spune că britanicul de rând este filmat în medie de până la 300 de ori pe zi, ceea ce face din Marea Britanie cea mai supravegheată societate de pe fața Pământului. De fapt, nu avem nici cea mai mică idee de câte ori intrăm în obiectiv fără voia noastră.

Știm că suntem filmați când călătorim cu trenul ori cu mașina, în supermarketuri, parcuri și bănci, când mergem la un meci de fotbal sau când folosim un bancomat, când facem exerciții într-o sală de fitness sau când intrăm într-un tribunal, când trecem prin centrul orașului ș.a.m.d. Dar niciunul dintre noi nu poate ști cu certitudine de câte ori suntem filmați, în secret, de poliție sau de serviciile secrete ori ilegal, de persoane fizice, din rațiuni financiare. Însă faptul că nu se pot furniza date precise privind supravegherea din umbră nu schimbă cu nimic lucrurile. Supravegherea oficială reprezintă un motiv suficient de îngrijorare, un exemplu în acest sens fiind camerele instalate în dreptul stațiilor de autobuz. Dacă ești atent când treci prin dreptul magazinelor pe orice arteră urbană aglomerată, îți vei face o idee în legătură cu cine sunt aceia care îți înregistrează plimbarea și din ce motive.

Cele mai multe magazine de desfacere fac parte din asociații care practică schimbul de informații. Când situația o impune, ele colaborează pentru a urmări anumite persoane pe perioade îndelungate și pentru a obține date digitale complete despre unde s-au oprit acestea pe durata plimbării lor pe strada în cauză. Există numeroase moduri prin care se poate urmări traseul unei persoane.

Kensington High Street din vestul Londrei, de pildă, este una dintre cele mai supravegheate străzi din capitală. Este o zonă de lux de vreun kilometru și jumătate, odinioară loc de promenadă al văduvelor înstărite și al pechinezilor acestora, în prezent un paradis al cumpărătorilor; aici se mai află sediul *Daily Mail* și al mai multor ambasade. Pornește de la Royal Garden Hotel și îndreaptă-te către Holland Park. Ridică-ți

privirea la zidurile din zona recepției hotelului și, undeva deasupra celor mulți care așteaptă să își primească ori să își predea camerele de hotel, vei vedea o jumătate de duzină de cutii negre suspendate. Aceste cutii ascund lentilele mobile ale unor camere de luat vederi comandate de la distanță.

Royal Garden este unul dintre hotelurile de top ale Londrei. Șefi de stat, oameni de afaceri străini, spioni, mercenari, celebrități înstărite și excentrice formează clientela obișnuită a hotelului. Odată ce se cazează, ei vor să aibă posibilitatea de a se relaxa în camerele lor și de a-și vedea liniștiți de treburi. În plus, doresc să se știe în deplină siguranță. Directorii celor mai mari hoteluri din lume se află în posesia mai multor secrete decât majoritatea oamenilor. Ei trebuie să satisfacă toanele președinților și dictatorilor, ale vedetelor de film, ale starurilor rock și ale scriitorilor împătimiți de băutură, precum și să păstreze confidențial tot ceea ce văd. De asemenea, ei trebuie să facă în așa fel încât oaspeții lor să simtă că nu au de ce să se mai teamă din momentul în care au trecut de portarul în uniformă de la intrare. De aceea, directorii trebuie să se asigure că toți cei care pătrund în hotel sunt filmați și că îi pot supraveghea atât pe oaspeți, cât și pe vizitatorii lor, până în momentul în care părăsesc incinta.

La est de acest hotel se găsesc Palace Avenue și Kensington Palace Green. Cochetul drum care duce la palatul Kensington este străjuit de o parte de grădinile Kensington și de cealaltă parte de grădinile Kensington Palace. Când ieși din hotel și privești către peretele estic, vei vedea răsărind, ca niște ochi și urechi, camere și senzori ce au rolul de a acoperi zona de acces către apartamentele regale. Partea superioară a zidului este prevăzută cu sârmă ghimpată, pentru a preveni tentativele de deteriorare a echipamentului electronic ori de cucerire a unei poziții strategice în timpul vreunei parade. Colțul acesta al Hyde Park a fost locul în care mulțimea îndurerată a ridicat munți de flori în zilele ce au urmat morții prințesei Diana. Iată un punct vulnerabil al Marii Britanii. Alte camere de filmat ne așteaptă peste drum, în Bar Cuba, unde oaspeții hotelului dau fuga pentru a se bucura de plăcerile

unui pahar de băutură mai ieftin.

Puțin mai la vest, grădinile Kensington Palace sunt păzite de gardieni în uniformă. Bulevardul străjuit de copaci este deschis publicului, dar nu poate fi parcurs de mașini, cu excepția celor cu număr de corp diplomatic, și este interzis tuturor muncitorilor care nu dețin o autorizație specială. Majoritatea misiunilor diplomatice importante se află aici, inclusiv Ambasada Rusiei, în capătul nordic. În fața unor clădiri s-au montat baricade antitanc, pentru a preveni atacurile cu mașini-capcană, iar farfuriile antenelor-satelit se înalță deasupra acoperișurilor, făcându-și loc printre ramurile platanilor. Bulevardul mărginit de copaci geme de camere de supraveghere și antene radio, în timp ce polițiști înarmați patrulează non-stop – un motiv temeinic pentru ca toți cei care se gândesc să recurgă la un protest în fața Ambasadei Japoniei să-și schimbe planurile.

Dacă decizi să te tratezi cu o cafea pe cealaltă parte a străzii Kensington High, la Barkers, cu marmura sa edwardiană, vei vedea fără îndoială tineri scriind la laptopuri ori vorbind la telefoanele lor mobile. La etaj, în impunătoarea clădire Northcliffe House, se află sediile publicațiilor *Daily Mail*, *Mail on Sunday* și *London Evening Standard*. Cu degajarea pe care ți-o dă practica îndelungată, jurnaliștii sunt în stare ca, de la birourile lor, să asculte și să vadă tot ce se întâmplă în cafeneaua de la parter și chiar în hotel. Supravegherea și securitatea sunt maxime și fățișe în birourile *Associated Newspapers*, personalul fiind filmat în mod curent prin televiziunea cu circuit închis. Gențile și servietele sunt percheziționate, iar toate birourile și coridoarele simt împânzite cu camere de supraveghere. Testarea sistemului reprezintă o practică notorie printre jurnaliști. Atunci când s-a promulgat legea care interzice armele de dimensiuni mici și cluburile de tir, unul dintre cei dintâi reporteri ajunși în clădire, în chiar ziua intrării în vigoare a noii legi, a adus în redacția de știri un uriaș revolver Webley Service (nefuncțional), susținând că l-a găsit în lift. Măsurile de securitate valabile pentru întreaga clădire s-au înăsprit la scurt

timp. Compania dispune de un personal de securitate redutabil, nu doar din pricina implicațiilor politice ale activităților pe care le desfășoară, ci mai ales din pricina secretelor pe care le deține, dar alege să nu le divulge. Informațiile reprezintă totul pentru un ziar de scandal cu difuzare națională și e un lucru bine știut că editorii și directorii companiei îi pot oricând distruge sau pune într-o lumină cel puțin nefavorabilă pe unii dintre cei mai puternici oameni din Marea Britanie.

Informațiile sunt, de asemenea, importante în josul străzii, la sucursala din Kensington a Marks and Spencer, unul dintre magazinele-cheie din Londra ale companiei. În fața sa, zeci de femei și copii se învârt încoace și încolo, formând un grup imprezvizibil și zgomotos. Provin din Europa de Est și vorbesc în limba lor. Copiii par a nu mai putea fi controlați, în timp ce femeile poartă *burka* lungi și văluri care le acoperă fețele. Ne vom întoarce la ei în curând.

Spre deosebire de alți comercianți, Marks and Spencer nu obișnuiește să atașeze etichete de securitate mărfurilor sale, bazându-se, în schimb, pe supravegherea video și pe agenți de pază în uniformă ori detectivi de magazin în civil. Este un sistem eficient. Rețeaua marilor magazine londoneze menține legături strânse între toate spațiile comerciale și raportează orice mișcare a unui grup de clienți considerați suspecti. Eficiența forței de securitate M & S și abilitatea sa de a acționa în cazul unui furt au fost testate și dovedite în timp. Când un grup de potențiali hoți de magazine ori de buzunare pleacă din Kensington, magazinele din Oxford Street îi așteaptă deja. Unitățile comerciale trebuie să se bazeze pe experiența și rețeaua de comunicare pe care le dețin, deoarece comunicarea din interiorul Poliției este considerată prea lentă.

Pentru mulți cumpărători pretențioși, magazinele din Kensington și Chelsea au un aer de respectabilitate neagresivă și un calm care le fac preferabile celor din Oxford, aflat la vreun kilometru și jumătate la nord-est, cu nebunia permanentă a reducerilor de acolo. Cu mult mai puțin evident este însă succesul lor în contracararea furtului organizat.

Această luptă este neîntreruptă, prin urmare, neîntreruptă este și supravegherea clienților prin mijloace electronice. Fiecare persoană este înregistrată intrând, ieșind și plimbându-se prin magazin. Suma, dar și planificarea *investită în sistemul de securitate* al Marks and Spencer este, fără îndoială, imensă, și ne-ar surprinde pe toți. Din punct de vedere strict comercial, camerele de supraveghere par toate la fel, dar munca de supraveghere înseamnă mult mai mult. Dacă intri în încăperile de monitorizare ale M & S, nu vei găsi un munte de ecrane și agenți de securitate plictisiți, așteptând să li se termine tura. Fiecare magazin are zeci de camere de supraveghere, ale căror imagini sunt urmărite de persoane cu o pregătire minuțioasă, pe cel mai performant ecran unic de mari dimensiuni de pe piață. Tehnologia este cunoscută sub numele de „neurală”, ceea ce înseamnă că aceste camere digitale sunt capabile să discearnă activitatea suspectă de cea obișnuită, transmițând-o apoi pe prima operatorului. Programul izolează porțiunea relevantă de înregistrare și îi acordă prioritate, astfel încât supraveghetorul să vadă imediat ce se întâmplă, să identifice persoanele suspecte și să cheme în ajutor personalul de securitate din magazin. Este rapid, eficient și incredibil de scump, dar acesta este viitorul supravegherii.

Dat fiind că poate izola anumite amenințări de tiparele altminteri acceptabile de comportament, supravegherea neurală revoluționează arta supravegherii electronice. Avantajele sunt multiple, nu în ultimul rând pentru că te scapă de grămezi de ecrane greu de administrat și de o cantitate enormă de informații confuze. S-a stabilit că durata medie a vizionării active, de către polițiștii londonezi experți în CCTV de la sediul din Wood Lane, a imaginilor camerelor de supraveghere nu a fost mai mare de 20 de minute. Nimic nu le scapă camerelor neurale și sistemului de „prevenire proactivă” pe care acestea se bazează, ce face ca informația primită să fie selectată și afișată pe monitoare. Tot ce apare pe monitorul neural este relevant. Unicul operator de care sistemul are nevoie pentru a funcționa lucrează izolat, într-un

centru de comandă departe de locul supravegheat. El sau ea stă într-o cameră cu dotări spartane și un singur ecran de perete, imens, pe care pot fi transmise imaginile, fiecare imagine cu codul ei de prioritate. Lumina este difuză, iar operatorul este așezat într-un confortabil scaun cu spătar înalt, în fața unei mese cu o grămadă de telefoane.

Acest sistem versatil are multe alte aplicații, pe lângă cele din sectorul comerțului. De pildă, închipuiți-vă o uriașă reședință englezească în stil georgian, întinsă pe mii și mii de hectare de pășune și păduri, cu grădinile înconjurate de un zid înalt de cărămidă și sârmă ghimpată, cu lățimea de trei metri la bază... Cele patru intrări principale în parc sunt controlate electronic. Terenul și pereții casei sunt împânziți cu camere de luat vederi și cu senzori de mișcare. Interiorul casei este dotat, de asemenea, cu mici camere ascunse, fiecare dintre acestea fiind setată pentru a opera cu un sistem programat în prealabil. Întregul material brut înregistrat de camere și de senzori este transmis unității de monitorizare la distanță, unde e filtrat și evaluat de către sistem. Fiecare cameră înregistrează și analizează activitățile care au loc într-un spațiu precis definit. Camerele pot detecta mișcarea, urmări și analiza comportamentul, pe baza sistemului integrat „extremitatea dinamică principală”. Acesta presupune ca, atunci când se sesizează o anomalie, oricare ar fi natura acesteia, detaliile să fie afișate în camera de control, unde operatorul sistemului, așezat în fața unui ecran de perete imens, cu o imagine foarte clară, poate activa calea cea mai indicată de acțiune.

Fiecare cameră este programată pentru a considera acceptabile o serie de activități care au loc în raza sa de acțiune. Orice a fost indicat ca reprezentând un comportament suspect este izolat și înregistrat, spre deosebire de restul tiparelor de acțiune. De exemplu, un bărbat care intră în parcare din spatele proprietății. El poartă o geantă pe care o lasă pe jos, lângă un alt autoturism parcat. Apoi se întoarce și pleacă, lăsând în urmă geanta. Sistemul interpretează imediat situația descrisă ca pe o amenințare și o retransmite

instantaneu către operator, care va trebui să o analizeze. Geanta este scoasă în evidență și prezentată hașurat pe ecran, astfel ca privirea care monitorizează să fie atrasă imediat de ea, iar operatorul să poată înțelege fără întârziere natura problemei. Sistemul îi furnizează o înregistrare video completă a momentelor care au precedat și a celor care au urmat incidentului, permițându-i să examineze în cele mai mici detalii atât geanta, cât și persoana care pare a fi abandonat-o.

Acest sistem se numește Spectiva. Înregistrările sunt atât audio, cât și video de calitate, existând posibilitatea izolării și redării unei conversații anume dintr-o zonă extinsă. Privitorul primește orice detaliu de care are nevoie pentru a lua decizia necesară analizării a ceea ce s-a înregistrat și să acționeze în consecință. Dacă persoana care a penetrat perimetrul înregistrării ar fi lăsat geanta jos doar pentru câteva momente, pentru ca apoi să o ridice și să își vadă de drum, sistemul ar fi putut fi programat să ignore incidentul. Sistemul de supraveghere a fost programat pentru a acționa în cazul unei game largi de posibilități sugerate de către firma de securitate care l-a instalat. De pildă, dacă, în timpul nopții, o siluetă aleargă prin parcare sau intră în raza de acțiune a camerei de supraveghere și se ghemuiește în spatele unei mașini, incidentul va fi selectat și afișat instantaneu operatorului. Dacă un copil aleargă în același loc ziua, ceea ce nu constituie în principiu nimic anormal, sistemul poate fi programat pentru a-l ignora. Dacă o persoană pare a purta o armă, camerele de supraveghere o vor recunoaște ca atare și vor reacționa în consecință. De îndată ce comportamentul în cauză a fost analizat, sistemul va continua urmărirea subiectului. Îmbrăcămintea neadecvată, o mască de schi sau o vestă antiglonț pot fi recunoscute, declanșând un răspuns corespunzător. Tehnologia recunoașterii faciale a făcut posibilă amplasarea camerelor în așa fel încât să permită stocarea conturului sau a caracteristicilor fizice ale tuturor vizitatorilor, cunoscuți și neinvitați, ai casei sau ai dependențelor. Totuși, tehnologia se află încă într-un stadiu

incipient de dezvoltare și poate fi contracarată prin folosirea unor articole de îmbrăcăminte sau a unor ochelari ce ascund chipul.

În cazul unei case particulare din mijlocul unui mare domeniu din Anglia rurală, prioritară este mai degrabă siguranța familiei și a proprietății, iar sistemul se poate să fi fost instalat la insistențele asigurătorilor familiei. Prima dată când m-am confruntat cu eficiența sistemului neural a fost la o casă particulară din Hampshire. Sistemul fusese instalat de către una dintre cele mai mari firme de supraveghere, CSS, cu sediul în Southampton. O mare plăcere a proprietarului casei a fost să-mi arate cum își poate monitoriza proprietatea oriunde s-ar afla în lume, prin intermediul laptopului sau al unui palmtop.

Bunăoară, aflat într-un hotel în Tokio, utilizând tehnologia wireless și propriul laptop, el poate comunica și controla camerele de supraveghere. Dacă vrea, poate urmări orice anomalie semnalată de sistemul neural. Instalația sa Cieffe, de proveniență italiană, oferă posibilitatea vizionării integrale a înregistrărilor pe un monitor virtual și a activării comenzilor de la mare distanță. Privind sistemul la lucru într-un bar din City, în compania proprietarului, am putut citi minuscula inscripție de pe autocolantul de plată a asigurării vehiculului, filmată de o cameră situată la 100 de metri de mașină, pe peretele posterior al casei. Pe de altă parte, facilitatea de a capta sistemul și de a recepționa imagini cu propria casă și cu membrii familiei este menită a servi exclusiv confortului psihic al proprietarului, deoarece sistemul este monitorizat 24 de ore pe zi de personalul CSS, cu care acesta poate intra în contact prin simpla apăsare a unui buton.

Înainte de a-l consilia pe proprietar, CSS a analizat vulnerabilitatea casei de la țară. Reprezentanții firmei au dotat sistemele complete, dar discrete, de detectare a încălcării perimetrului, cu CCTV proactiv, care transmite semnale unui dispecerat central. Compania folosește serviciile unor operatori cu experiență, care pot răspunde pe loc oricăror amenințări la adresa casei sau a bunurilor din



interiorul acesteia. Robert Fiorentino, responsabilul CSS în Southampton, proiectează sisteme de securitate la comandă. „Putem face ceea ce Poliția este adesea incapabilă să facă, adică să protejăm locații vulnerabile și să prevenim infracțiuni grave”, a declarat el. De exemplu, în cazul unui atac de proporții asupra unei proprietăți, informațiile sunt selectate de către sistem și afișate pe ecran într-o selecție de imagini prioritare, dându-i astfel operatorului suficiente amănunte pentru a-și putea face o imagine completă asupra incidentului. În calitate de agenție privată, CSS nu este condiționată de sistemele puternic birocratizate de raportare a datelor, dar respectă Legea protecției informațiilor, precum și orice alte legi și regulamente care normează furnizarea dovezilor în cadrul unui proces. Tehnologia neurală utilizată în supraveghere este privită în industrie ca fiind mai degrabă preventivă decât reactivă – un important pas înainte în securizarea proprietății.

Scopul dintâi al sistemelor precum cel proiectat de CSS este de a preveni infracțiunile săvârșite în spații publice. În SUA, eforturile de a stabili o legătură între căutarea neurală, detectarea și supravegherea mișcărilor, pe de o parte, și tehnici precum recunoașterea facială și tehnologiile sateliților de poziționare globală (GPS), pe de altă parte, sunt în desfășurare de mai bine de doi ani, în cadrul unei inițiative a Departamentului de Securitate Internă. Obiectivul este dezvoltarea unui sistem care se poate aplica pe o stradă aglomerată, pentru prevenirea unui posibil atac terorist.

Tehnologiei supravegherii neurale i se aduc permanent îmbunătățiri, prețul acesteia scade constant, iar personalul însărcinat cu operarea sistemului are parte de o pregătire din ce în ce mai sofisticată. Nu peste mult timp, acest sistem va ajunge să fie folosit de toate marile magazine, iar informațiile pe care le furnizează vor fi coroborate cu cele ale bazelor de date ale infractorilor cunoscuți. Nu ar trebui să ne mire interesul comercianților pentru dezvoltările aplicațiilor de securitate care oferă facilitatea de a selecta imaginile, reducând astfel personalul angajat. În perioadele aglomerate,

la sfârșit de săptămână, marile magazine din West End devin câmpurile unui război comercial de gherilă, informațiile privind infractori cunoscuți sau suspecti fiind transmise, de la un distribuitor la altul, în întreaga zonă. La orele de vârf, echipajele de poliție patrulează de-a lungul străzii și în stația de metrou. În lunile de vară, magazinele din Kensington sunt vizitate regulat de grupuri de hoți, printre care mulți veniți din Europa de Est și Balcani. Aceștia acționează în grupuri mici. Linia de atac este formată adesea din femei și copii, ajutați de bărbați care conduc mașini rapide, în susul și în josul străzii. Fetele și băieții prepuberi implicați sunt antrenați intens, pentru a deveni ași ai furtului de buzunare (altfel spus, ai „ciordelii”), pentru a învăța cum să păărăsească locul faptei și să distragă atenția victimelor. Au asupra lor identități false, pentru a-i convinge pe polițiști și pe detectivii de magazin că sunt minori, pretinzând de asemenea că nu cunosc limba engleză. Operează în echipe și sunt foarte îndemânatici. Traseele lor de retragere sunt stabilite minuțios și repetate conștiincios.

În încercarea de a contracara amenințarea hoților din magazine, de îndată ce apare cel mai mic indiciu al unui incident sau un infractor cu cazier este recunoscut, sunt alertați pe loc toți comercianții de pe stradă, precum și unitățile poliției de combatere a furturilor din magazine din Kensington și Notting Hill. Mai multe lanțuri mari testează în prezent supravegherea pe baza recunoașterii faciale, ca mod de a identifica și de a lua măsuri împotriva hoților profesioniști. Deși este mană cerească pentru sistemele de securitate, identificarea facială mai are încă mult până să-și dovedească infailibilitatea.

În prezent, Londra este cel mai supravegheat oraș din lume. Pe lângă cele două milioane de camere cu circuit închis, există opt elicoptere de supraveghere ale poliției – și alte două în pregătire –, prin intermediul cărora se pot transporta rapid, practic oriunde în capitală, echipaje înarmate. În funcție de gradul de vulnerabilitate, s-au format zone de securitate, unele supravegheate mai intens decât altele. Polițistul cu

baston și fluier care patrulează pe stradă a devenit un exponat de muzeu. Urmașul său modern este dotat cu motocicletă rapidă, sisteme de comunicare de ultimă oră și echipament atât defensiv, cât și ofensiv.

Sistemul chiar funcționează. Recent, am însoțit doi polițiști pe bicicletă ai Poliției londoneze în Aldersgate, unde ei au observat un domn mai în vârstă, mergând hotărât în direcție sudică. „Îl cunosc”, a spus unul din tovarășii mei, un sergent musculos, îmbrăcat în galben reflectorizant, cu vestă antiglonț și spray paralizant, baston, pistol cu electroșocuri și trusă de prim ajutor., „Blochează telefoanele publice cu bucăți de plastic și se întoarce mai târziu pentru a strânge banii; l-am mai săltat acum vreo câțiva ani”. El a luat legătura cu unitatea de monitorizare prin televiziune cu circuit închis, cu ajutorul radioului încorporat în cască, „E un bătrân în impermeabil galben, care se plimbă prin Aldersgate, la vreo 45 de metri sud de Long Lane, îl vedeți pe ecran?” După nici 20 de secunde, bărbatul era urmărit prin intermediul camerelor, în prim-plan și cu maximum de detalii, din camera de supraveghere de pe Wood Street. L-am urmărit de la distanță, în timp ce camerele de supraveghere îl înregistrau cum a luat-o pe Grubb Street și apoi pe Cheapside, unde s-a oprit pentru a se uita la o vitrină. Polițiștii s-au dus să îl întrebe de sănătate, în timp ce eu priveam. Un al treilea polițist pe bicicletă, o femeie sergent, s-a înființat și ea lângă ei, pe trotuar, deși n-aș putea spune de unde apăruse. După alte câteva minute, un alt polițist a apărut la fața locului. Din senin, strada se umpluse de polițiști pe bicicletă.

Nu am asistat la comiterea vreunei agresiuni, polițiștii au fost toți amabili și politicoși, însă asta după ce îl urmărisem pe acel bărbat preț de 30 de minute și după ce acesta fusese filmat în ascuns și cu mare acuratețe, din Aldersgate până în Cheapside. Susținea că muncește în Finsbury Square și că are tabietul de a ieși la plimbare în fiecare zi, la ora prânzului. Însă omul nu se afla la prima confruntare cu poliția și, după cum a spus apoi unul dintre oamenii legii, „dacă în viitor va mai dori să facă ceva necurat, o să se gândească de două ori

înainte. Îi știm numele și adresa”. Asta mai însemna că acest incident minor fusese înregistrat și că trăsăturile faciale ale bărbatului fuseseră stocate în baza de date apoliției, de unde, printr-o singură apăsare a unei taste, puteau fi reactualizate și adăugate în baza lor de date de recunoaștere facială. Protagonistul acestui episod neînsemnat, dar antrenant, nu avea nici cea mai vagă idee că plimbarea lui de prânz tocmai fusese înregistrată pentru posteritate sau că propria figură putea fi afișată pe un ecran de computer nu numai din Londra, dar în curând și din orice stat cu care s-au semnat acorduri în domeniu, chiar și după ce el va fi fost de mult oale și ulcele.

Sistemul de supraveghere din City, cu program de recunoaștere automată a numărului de înmatriculare, va fi în curând implementat în 23 de secții din Anglia, iar apoi în toată Marea Britanie. Teoretic, sistemul va fi utilizat la scară națională pentru a monitoriza cele opt milioane și jumătate de mașini pentru care nu s-au plătit taxe, neasigurate ori suspectate de a fi utilizate pentru infracțiuni sau terorism. Camerele pot monitoriza în prezent 3.500 vehicule pe oră și vor fi instalate atât în locuri fixe, cât și montate pe dubele poliției. Însă nu există absolut nicio garanție a faptului că utilizarea sistemului se va limita la găsirea „adevăraților” infractori.

Tehnologia de supraveghere este îmbunătățită permanent. Deja nimic nu poate opri poliția și serviciile secrete de la a conecta sistemul la baza de date a Autorității pentru Șoferi și Autovehicule (DVLA), în care se regăsesc numele și adresa fiecărui posesor de mașină din țară. Aceasta nu numai că ar accelera ritmul arestărilor pentru neplata parcării sau a amenzilor pentru depășirea limitei de viteză, dar ar facilita și urmărirea traseului zilnic al șoferilor. Pericolul la adresa libertăților cetățenești rezidă în aceea că încurajează poliția și, implicit, statul să înregistreze tiparele noastre de comportament și, pe baza înregistrărilor, să tragă concluzii.

În timp ce City-ul reprezintă probabil unul dintre peisajele urbane cel mai intens supravegheate și păzite din lume,

Kensington Street nu diferă prea mult de orice altă arteră importantă a Marii Britanii. Mergi pe Kensington și sigur vei fi permanent supravegheat de vreo cameră. Intră într-un magazin sau într-un restaurant și vei fi preluat de un alt sistem de supraveghere. Pretutindeni în jurul tău se desfășoară această luptă între comercianți și infractori, iar tu te afli, fără voia ta, în mijlocul ei, doar pentru că te-ai nimerit pe acolo și vrei să cheltuiești niște bani. Prin lege, imaginea ta ar trebui ștearsă din sistem în termen de 31 de zile, însă nimeni nu este desemnat să verifice dacă acest lucru se și întâmplă. Când îți folosești cartea de credit pentru a-ți plăti cumpărăturile și îți arăți cardul de fidelitate la casă, tranzacția durează suficient pentru ca imaginea ta înregistrată să poată fi corelată cu detaliile cardurilor tale. Proprietarii magazinului pot afla cu ușurință unde trăiești, ce servicii bancare utilizezi, câți copii ai și încă multe altele, prin simpla confruntare a înregistrărilor de pe camerele de supraveghere cu cele din rapoartele casierilor.

Astăzi nici pe stradă nu trebuie să vorbești ce nu trebuie, pentru că tot ce spui poate fi interceptat prin telefonul tău mobil, analizat și catalogat drept opinie personală, astfel încât te poți trezi trecut pe lista de persoane considerate indezirabile de către stat. Și nu trebuie să te temi doar de serviciile secrete, ci și de mass-media din Marea Britanie. „Conversațiile private” de altă dată, acelea pe care nimeni altcineva nu le mai putea auzi, au devenit un vis frumos. Nu mai există legătură telefonică sigură, internetul se oferă larg interceptării, iar e-mailurile au devenit bun comun. Dacă nu cumva stai lângă o cascadă, protejat de un cordon de agenți de securitate surzi, care au fost percheziționați pentru a nu purta cu ei dispozitive de înregistrare și care formează în jurul tău un cerc cu diametrul de cel puțin 200 de metri, atunci nu ai nicio garanție că discuția confidențială cu prietenul tău sau cu nevasta acestuia va rămâne între voi. Șeful MI5 comunică cu prim-ministrul prin intermediul unor informări scrise de mână și livrate personal de către un curier la Camera Comunelor. Chiar dacă îți iei toate măsurile de precauție

posibile, tot nu poți băga mâna în foc pentru confidențialitatea unei comunicări.

Se prea poate ca un dispozitiv de înregistrare audio sau de monitorizare a mișcării să fi fost instalat în podea sau în vreun tufiș din apropiere. E la fel de posibil ca un satelit să te filmeze sau ca un aparat aeropurtat în miniatură fie să te asculte, fie să îți înregistreze mișcările gurii, pentru ca apoi să le traducă în cuvinte.

Telefoanele mobile sunt interzise în cluburi private, în săli de judecată, în unele întruniri de afaceri și politice nu doar pentru că sunt iritante, ci pentru că pot fi prevăzute cu camere care pot filma sau fotografia ori cu funcții de înregistrare audio. Cele mai multe telefoane mobile moderne sunt suficient de avansate pentru a înregistra conversații din vecinătate. Dispozitive miniaturale, digitale, cu activare la voce, cum este Olympus DS330, pot fi cumpărate în Londra, pe Tottenham Court Road, cu 100 de lire sterline. Ascunse în buzunar, ele pot înregistra conversații într-un local zgomotos, eliminând sunetele nedorite de fundal. Dacă rețelele de supraveghere și interceptare a convorbirilor sunt supuse Legii protecției datelor și legislației privind drepturile omului, nimeni nu poate ști câte persoane private ori companii utilizează astfel de dispozitive pentru a înregistra activitățile pe care le derulezi. Câte hoteluri efectuează regulat controale de siguranță pentru a depista eventualele camere de supraveghere ori microfoane? Aproape niciunul. Dacă soliciți servicii de această natură marilor hoteluri londoneze, ei vor angaja o echipă de specialiști. Dar asta numai dacă o ceri în mod expres și, oricum, la un preț prohibitiv. Desigur, ei ar prefera să îți rezolvi singur problema, dat fiind că nu pot garanta siguranța antiinterceptare a camerelor și, dacă într-adevăr ești înregistrat, atunci hotelului i s-ar putea imputa daune. Și cât de des ar trebui să fie controlată camera ta? Zilnic? De două ori pe zi? Poate cineva garanta că firma de securitate angajată să-ți verifice dormitorul este destul de eficientă pentru a depista lentilele din fibră optică aflate probabil în spatele oglinzii de la baie? Dar dacă lucrează

pentru altcineva? Chiar și o verificare internă s-ar putea dovedi insuficientă. Dispozitivele de ascultare cu rază lungă de tip Sentinel pot fi îndreptate către fereastra unui dormitor, transformând vibrațiile percepute în unde sonore. Și, în fond, cum îl poți împiedica pe un jurnalist echipat cu cele mai scumpe dotări disponibile în comerț să-ți asculte conversația, dacă el chiar ține morțiș să o facă? Patronii săi dețin resursele pentru a achiziționa echipamente mai sofisticate decât cele la care ar putea visa vreodată serviciile de informații.

Elizabeth Hurley, ca orice vedetă, a avut multe probleme de acest gen. „Personal, nu cunosc nicio celebritate căreia să nu îi fi fost ascultate convorbirile”, a declarat ea recent. „Toți caută permanent și pretutindeni microfoane. Asemenea traficantilor de droguri, toți avem telefoane pe bază de amprentă digitală, fără număr înregistrat, însă mi s-au interceptat inclusiv convorbirile la telefonul fix, așa că acum nu mai vorbesc la telefon. Dacă vreau să mă întâlnesc cu cineva și să am o conversație privată, atunci întâlnirea va avea loc pe un pod. S-a ajuns până la a mi se planta microfoane în camera de hotel. Sunt bani buni la mijloc pentru acești ratați care nu știu cum altfel să câștige o pâine”.

Interceptarea convorbirilor celebrităților nu este o invenție de dată recentă. Koo Stark mi-a mărturisit, la un moment dat, că i s-a ascultat telefonul în perioada în care era partenera ducelui de York. „Știam că cineva ne asculta convorbirile, deoarece *Daily Mail* a publicat detalii ale unei conversații care nu puteau fi obținute altcumva. Era o problemă gravă, fiindcă știam că dispozitivul nu fusese montat în casă, așa că serviciul de pază a trimis experți în supraveghere, iar ei au dezgropat un microfon pe linia telefonică terestră din dreptul casei, cam la 20 de metri de locuința mea, într-un grajd aflat la nord de Belgrave Square. Știam cu siguranță că aceasta reprezintă una din măsurile de supraveghere puse la cale de David English de la *Daily Mail*. Ar fi făcut orice să afle până și cel mai nesemnificativ amănunt despre noi. Este oarecum bizar, dar, când îți dai seama că ai fost urmărit, devii foarte precaut în privința locurilor unde vorbești cu oamenii. Nicăieri nu mai

ești în siguranță”.

Celebritățile ar deveni încă și mai paranoice – și pe bună dreptate – dacă ar ști că deseori polițiștii simt aceia care furnizează informații reprezentanților mass-media. La începutul lui 2005, o rețea de foști polițiști londonezi, incluzând un operator al sistemului de supraveghere și mai mulți detectivi particulari, a fost condamnată pentru vânzarea numerelor de înmatriculare ale unor vehicule, precum și a unor date obținute de la Biroul de Informații privind Infractorii (CRO – Criminal Records Office). Datele transmise includ detalii privind mai multe vedete de televiziune, precum și detalii cu privire la infracțiunile rutiere comise de conducătorul unui autocar implicat într-un accident pe teritoriul Franței. Deși aceste date nu par a avea cine știe ce greutate, ele au servit la susținerea unor articole speculative apărute în ziare de scandal. Aceasta reprezintă o demonstrație a faptului că e extrem de ușor să încalci regulile, și că o informație altfel minoră poate fi utilizată pentru a da o spoială de veridicitate unui articol prost documentat, astfel încât acesta din urmă să poată fi publicat. De pildă, detalii privind proprietarul unui scuter folosit de un lider sindical pentru a circula în Londra în timpul grevei angajaților de la metrou au fost transmise lui Paul Marshall, responsabil cu relațiile publice la o secție de poliție din sudul Londrei, care le-a oferit lui Alan King, fost polițist, iar acesta, la rândul său, le-a vândut unui jurnalist. În timpul procesului, judecătorul a apreciat că siguranța informațiilor clasificate depinde de buna-credință a numărului mare de polițiști care le manipulează. Procesul, care s-a ținut la Tribunalul Regal Blackfriars, unde cei patru acuzați au fost condamnați, a demonstrat că există o piață largă de desfacere pentru materialele secrete aflate în posesia poliției. Cererea va crește odată ce baza de date computerizată a poliției va deveni mai mare și mai accesibilă hackerilor și cyberteroriștilor.

Așadar, în timp ce ți-ai făcut cumpărăturile pe Kensington, ai fost filmat, iar tranzacțiile pe care le-ai derulat au fost înregistrate. A sosit timpul să te întorci acasă. La stația de



metrou Kensington High Street, ușă în ușă cu Marks and Spencer, 25 de camere înregistrează tot ce intră și iese. Când pasagerii se înghesuie să treacă de turnichet, folosind cardul de transport în comun, ei lasă în urma lor o amprentă care nu poate fi ștearsă. Polițiștii de la Transporturi și cei de la secția din Kensington de pe Earls Court Road se amestecă printre navetiști. În timp ce îi caută pe hoții de buzunare care se pierd în vasta rețea subterană, ofițerii de la fața locului primesc permanent date de la cei care monitorizează camerele de supraveghere, prin intermediul frecvenței radio alocate poliției.

Un tur pe orice stradă aglomerată suscită automat o senzație de nervozitate acută, de îndată ce îți dai seama de numărul semnalelor și urmelor care plutesc în aer, deasupra ta. De fiecare dată când folosești o carte de credit, un „card inteligent” sau un telefon mobil, de fiecare dată când dezactivezi sistemul de închidere a mașinii cu telecomanda, poziția ta exactă pe hartă poate fi stabilită și înregistrată, iar mișcările și acțiunile tale pot fi urmărite cu maximum de acuratețe. Mergi pe o stradă din vestul Londrei și vei putea observa senzorii care absorb și transmit informațiile către baze de date publice și private. Odată înregistrate informațiile, ele pot fi transmise instantaneu poliției, serviciilor secrete și firmelor de pază. Ampretele electronice pe care le lăsăm în urma noastră ne-au schimbat pe veci viața. Totuși, cei mai mulți dintre noi nu suntem conștienți că nu am mai trăit niciodată într-un astfel de mediu.

În industria computerelor, există o maximă cunoscută sub numele de Legea lui Moore, care spune că performanțele computerelor se dublează la fiecare 12 luni. Așa că vor exista destule pârghii de silicon pentru a procesa și a analiza chiar toate datele personale. Iar acum că *Ei* dețin informațiile, ce vor face cu ele? Și totuși, cine sunt *Ei*?

## Capitolul II

### Ei îți marchează cardul

*Patronii magazinelor nu se bazează numai pe camerele de supraveghere pentru a afla diverse lucruri despre noi, în timp ce ne plimbăm printre rafturi sau ne plătim cumpărăturile la casele de marcat suntem participanți benevoli la goana lor după informații, deoarece le oferim toate datele de care au nevoie pentru a construi un raport meticulos despre noi – și o facem pentru nimica toată, an după an. Le permitem să își dea seama cum ne afectează publicitatea obiceiurile de cumpărători, cât de sensibili suntem la creșterea prețurilor, la ofertele cu reduceri, la lansarea unor noi produse și la modul de aranjare a mărfurilor în magazine. Ei află dacă suntem bărbați sau femei, singuri sau într-o relație, tineri sau bătrâni, purtători ai unei sarcini sau deja părinți, sportivi sau sedentari. Industria ne încurajează să ne vindem intimitatea pentru o reducere de 1%. Și, pe măsură ce ne assemblează un portret detaliat în bazele lor de date, ei află mai multe despre noi decât știe guvernul.*

Mama mea a murit la o vârstă înaintată și, după aceea, în timp ce îi umblam prin maldărele de obiecte personale și îi scotoceam poșetele, am descoperit că avea în portofel șase carduri de fidelitate de la niște supermarketuri. Știam că îi plăcea să le folosească. În ultimii ei ani de viață, o scoteam la cumpărături la fiecare sfârșit de săptămână, deoarece, pentru ea, asta era o zi de vacanță. După ce găsea fiecare lucru de pe lista ei de cumpărături și porneam spre casa de marcat, fata de la teighea o întreba dacă era „o membră a clubului”, iar mama mea făcea mare caz din a-și căuta cardul și a i-l înmâna. Accepta cardurile din două motive. Mai întâi, simțea

că, dacă n-ar fi avut un card, ar fi pierdut ceva; în al doilea rând, îi plăcea să creadă că aparține unui club. Nu a cerut niciodată vreuna dintre reducerile care i se cuveneau, din câte știu eu. Nici măcar nu cred că citea scrisorile pe care le primea de la magazin. Dar ea făcea parte dintr-o generație pentru care cumpătarea era o virtute, iar colecționarea punctelor-bonus – un mod de a economisi bani, chiar dacă, de fapt, nu le solicita niciodată. Era datoră ei să fie prudentă. Atitudinea ei relaxată față de toate astea nu era reflectată de comercianți, pe care i-a susținut de-a lungul întregii sale vieți.

La sfârșitul vieții, frații și surorile îi muriseră de mult și avea doar familia apropiată și îngrijitorii care să-i țină de urât. Am descoperit că, timp de ani întregi, ea păstrase toate scrisorile primite, pe care le ținea în cutii. Era, în cea mai mare parte, o colecție deprimantă de corespondență bună de aruncat la gunoi, acceptări personalizate ale cererilor ei inexistente de carduri de platină „gratuite”, nenumărate oferte de împrumuturi, „sugestii folositoare” de a face o ipotecă pe casă în schimbul unei croaziere în jurul lumii sau al unei noi sere și multe altele de genul acesta. Săptămână după săptămână, an după an, ofertele au curs în valuri. Și, desigur, au fost nenumăratele ocazii în care a câștigat „un premiu consistent în bani”. Tot ce trebuia să facă pentru a-l ridica, fără niciun fel de obligație, era „să sune la acest număr”. Mai jos, cu caractere mult prea mici pentru a putea fi văzute de ochii ei bătrâni, scria: „Apelurile se taxează cu cinci lire pe minut, pentru primele trei minute”. Nu a fost păcălită de niciuna dintre aceste șarlatanii, deși, în fiecare an, mii de femei bătrâne cad în capcană. În timp ce parcurgeam mormane de oferte înzorzonate, m-am trezit întrebându-mă ce măsuri de protecție există pentru cei bătrâni și vulnerabili și cine se ocupă de apărarea intimității lor.

Cine știa unde locuiește și că era o proprietară în vârstă? Se știa că nu avusese niciodată datorii, în lunga ei viață? În afară de familia ei apropiată, oamenii care știau cele mai multe lucruri despre ea erau patronii magazinelor pe care le vizita. Asta deoarece, cu ani în urmă, completase cereri pentru

cardurile lor de loialitate și, făcând asta, își divulgase toate datele personale. Continuase apoi să le dea informații, fără a avea nici cea mai vagă idee că ceea ce scrie pe formular avea să ajungă mai departe. Milioane de oameni pleacă urechea la sloganurile: „Fiecare mărunțiș contează”, „Știi că are sens”, „Ai grijă de penny și lirele vor avea singure grijă de ele”, „Păstrează și vei avea” sau ”Paza bună trece primejdia rea”. Doar una dintre aceste axiome moralizatoare nu e o rămășiță a înțelepciunii casnice victoriene, și aceea e prima. „Fiecare mărunțiș contează” e, de fapt, un crâmpiei isteț de text publicitar, care definește filosofia cardului de loialitate al Clubului Comercianților, o extravagantă de marketing și de colectare de informații, pe care compania o descrie, grandios, drept un „întreg concept”. Un „club de loialitate” standard din comerț îmbrățișează sentimentul călduros al apartenenței la un club, ajutându-ne în același timp să economisim bani. O viață de cumpărături însumează sute de mici bonusuri, în special dacă mergem la același supermarket pentru tot ceea ce avem nevoie și dacă putem răspunde „da” la toate întrebările sâcâitoare: „Aveți un card de magazin Tesco / Safeway / Boots / Marks and Spencer / Target / Metro?”, de fiecare dată când dăm o fugă să cumpărăm un kilogram de cârnați. Poate că îți folosești cardul Nectar la Sainsbury's, Debenhams, BP și Vodafone, caz în care aproape orice tranzacție comercială pe care o vei efectua de-a lungul vieții ar putea să îți aducă puncte. Și ce înseamnă punctele? Simplu spus, PUNCTELE ÎNSEAMNĂ PREMII.

Desigur, nu e chiar așa de simplu. Postează-te la casa de marcat din orice mare supermarket și privește înjur. Acesta e un spațiu amplu și forfotitor, proiectat cu grijă pentru a deveni un colț familiar și prietenos al lumii tale. Alimentele sunt însumate pe bon și achitate, poate, cu cardul tău Visa. Fidelitatea îți e recunoscută cu o trecere a cardului peste senzor și cu un zâmbet din partea fetei de la casă, apoi îți împingi căruciorul cu produse cumpărate spre mașină, pe lângă agentul de securitate și pe lângă senzorii antifurt. Nu vrei să știi că undeva, deasupra ta, tranzacția a fost filmată

prin televiziunea digitală cu circuit închis, plata a fost înregistrată și cronometrată, iar imaginea trupului și a feței tale au fost înregistrate în baza de date, cu detalii despre cardul de loialitate. Magazinul deține acum aspecte ale identității tale care ar face orice polițist din serviciile secrete să rânjească invidios.

Cardurile de fidelitate sunt forma rafinată și modernă a timbrelor Green Shield, un sistem de a economisi bani lansat prin anii 1950. În acest sistem, primeai timbre Green Shield ori de câte ori făceai o achiziție și le lipeai într-un album, până când aveai suficiente pentru a le răscumpăra. Cu cât economiseai mai mult, cu atât mai mare era recompensa. Timbrele Green Shield erau bune, deoarece te învățau să faci economii și să fii cumpătat, și erau reconfortante, deoarece, pe atunci, colecționarea timbrelor era un hobby popular, pe care toată lumea îl înțelegea. Colecționarea timbrelor era un lucru bun și pentru Green Shield, pentru că își vindeau micile timbre supermarketurilor și ofereau recompensele. Problema cu timbrele Green Shield era că, pe atunci, comercianții obțineau foarte puțin din vânzări, în afara loialității clienților, și cu toții știm că nu există cadouri pe degeaba. În cele din urmă, negustorilor de alimente le-a picat fisa că puteau economisi bani răsplătind chiar ei loialitatea clienților și îngropând cheltuielile în bugetul de marketing. După care și-au dat seama că nu doar vor economisi bani, dar, ci și că prin înregistrarea tranzacțiilor într-un computer central, vor construi o bază de date cu preferințele de cumpărare ale clienților, care va deveni, cu trecerea timpului, o resursă neprețuită.

Conceptul de carduri de fidelitate pare foarte generos. Întreprinderea îți obține loialitatea, iar tu îți primești punctele, milele aeriene sau voucherele. Din păcate, e puțin mai complicat de atât. Dacă, de exemplu, te muți în comitatele din jurul Londrei și mergi la cumpărături la Shopco de trei ori pe săptămână, ți se va aduce mereu la cunoștință că deținerea unui card al clubului te va copleși cu beneficii din belșug. Nu te vei putea abține să nu intri în club și vei căpăta,

curând, obiceiul de a prezenta cardul de fiecare dată când mergi la cumpărături. Fiecare casă de marcat din fiecare magazin este conectată la baza de date a clubului, iar rezultatul e că fiecare coș cu provizii pe care îl cumperi este înregistrat și cercetat, până când se va fi construit o imagine detaliată asupra ta. Dacă ți s-ar prezenta această analiză a ta, după câțiva ani de „loialitate”, ar fi posibil să ți se pară alarmantă, dacă nu defăimătoare. Dar nu poți face mare lucru. Tipii în costume din clădirile opace de birouri ale cartierului general transformă faptele indiscutabile, spicuite din coșurile tale de cumpărături, în carnea și oasele propriilor creații. În ceea ce-i privește, ești ceea ce cumperi, iar profilul pe care îl creează, pe baza cardului tău, este precis până la ultimul cub de bulion.

Când depui cererea pentru cardul lor de loialitate, ți se dă un „Acord” care garantează că datele tale private sunt în siguranță la Shopco. De asemenea, ți se promite că, dacă precizezi că nu vrei să fii contactat pentru studii de piață, nu te vor deranja. Ei mai afirmă că se supun Legii protecției datelor (ceea ce, oricum, reprezintă o obligație prevăzută prin lege). Formularul tău de cerere presupune să completezi detaliile personale, inclusiv numele, adresa, vârsta ta și a tuturor celor care trăiesc la aceeași adresă. Mai trebuie să completezi și detalii legate de gospodărie, necesități dietetice și informații de contact, inclusiv adresa de e-mail, numărul de telefon mobil ș.a.m.d.

În schimb, ți se va trimite un card care îți va permite să câștigi un punct pentru fiecare liră sterlină cheltuită în magazin și vei putea să profiți de oferte speciale pentru noi linii de produse, plus puncte de bonus. Cumpără „Online” și vei face economii chiar mai mari. Fiecare punct pe care îl câștigi valorează un penny sau 1% și poți alege să îți ridici recompensele imediat ce acestea devin disponibile sau ori de câte ori te hotărăști să le încasezi. Poți să le lași să se adune ani întregi, dacă așa ai chef. Sunt oameni înregistrați în bazele de date ale supermarketurilor cu mii de lire sterline, adunate sub forma punctelor de recompensă care li se datorează. Care-

i clenciul? Punctele nu stârnesc interes. În baza de date a corporației American Express există cecuri de călătorie emise, încă nefolosite la ani buni după ce vacanța pentru care au fost eliberate a devenit de mult doar o amintire îndepărtată. Din punctul de vedere al Amex, acesta e un lucru neprețuit. Cecurile de călătorie, în sine, nu aduc profit, în timp ce banii plătiți pentru ele sunt investiți de Amex și aduc beneficii de 6% sau chiar mai mult.

Nu ești obligat, însă ar trebui să câștigi 150 de puncte ale clubului Shopco în timpul fiecărei perioade de colectare, care durează, fiecare separat, cam trei luni. Cardul încurajează și glorifică fidelitatea, ceea ce e un lucru bun pentru Shopco și îl face pe client să se simtă bine față de sine însuși și liniștit că magazinul este un element sigur, demn de încredere și prietenos în viața sa. Ia-ți un card și, de-a lungul anilor, informația pe care acest mic petic de plastic o transmite, codat, la Shopco, prin intermediul teighelei și prin baza de date, devine spionul din portofelul tău, care înregistrează cum îți trăiești viața și trage concluzii pe baza obiceiurilor tale de cumpărător. Nu le va spune analiștilor din cartierul general Shopco din Hertfordshire doar că ai un animal de companie, porți proteză dentară sau suferi de flatulență. Aplicând niște programe socio-demografice complicate la stilul tău de viață și la cel al altor 20 de milioane de clienți, ei vor fi în stare să stabilească stadiul existenței pe care tu – și alții din gospodăria ta – l-ați atins. Stilul tău de viață va influența tot soiul de produse vândute prin cele 3.000 de magazine ale Shopco. Obiceiurile tale de cumpărător vor fi transmise celor care produc mâncarea animalului tău de companie, adezivul tău pentru proteză și ceainicul tău electric. Pornind de aici, Shopco va face presupuneri despre mărimea venitului tău, despre pasiuni și preocupări, despre ceea ce obișnuiești să bei, despre atitudinea ta față de viața sănătoasă, despre activitatea ta sexuală, despre nivelul de educație și despre surplusul de venit, și îți va stabili poziția pe firmamentul socio-economic potrivit tehnicienilor de la cartierul general Shopco Megacorp. Vor ști când îți schimbi domiciliul, când mergi în vacanță,

când ești bolnav și când vei avea un copil.

Dar asta e încă în regulă. Până la urmă, sunt doar simpli băcani și tot ceea ce urmăresc sunt banii. Sau, nu e așa? Când te muți și-ți schimbi adresa de pe card, sunt mari șanse să primești un mic dar cu vouchere alese în mod special pentru un nou proprietar de casă (poate niște produse de curățat), împreună cu o listă de adrese și de numere de telefon ale magazinelor locale. Nivelul generozității va corespunde statutului tău în baza de date. În ceea ce privește descoperirea că a sosit un nou copil, ronțăitorii de cifre vor ajunge să-și dea seama de acest lucru din modul în care îți modifici profilul cumpărăturilor. Brusc, scutecele de unică folosință și laptele praf vor apărea drept achiziții regulate în baza ta de date. Poate că te vor invita să intri în Clubul Sugarilor din compania lor? Sună, într-adevăr, foarte fermecător, în lumina asta. Industria de retail deține, în prezent, vaste cantități de informații de acest gen despre noi.

Pretextând că vor să-și îmbunătățească randamentul și serviciile pe care le oferă clienților, comercianții au creat bănci de informații care s-ar dovedi neprețuite pentru tot felul de grupuri, inclusiv pentru multe cărora, mai mult ca sigur, nu ai dori să le împărtășești detaliile personale. Problema, în acest caz, este că nu vorbim despre date bancare. Sunt detalii ale clienților adunate de comercianți. Dacă un băcan observă că poate profita de pe urma unor resurse precum datele cardului de loialitate, va fi tentat să o facă. Dar cine știe unde ar putea ajunge aceste informații? Supermarketurile americane au oferit, de bunăvoie, FBI-ului amănuntele despre cardurile lor de fidelitate, după 9/11. Acceptabil, s-ar putea spune – aceea a fost, într-adevăr, o situație de criză. Da, dar a fost și începutul unei afaceri foarte grase. A înlesnit transmiterea datelor spre politicieni pe care s-ar putea să nu-i sprijini și care nu ai vrea să-ți cunoască detaliile personale. Clienților din bazele de date ale supermarketurilor nu li s-a spus niciodată că informații despre ei au fost oferite guvernului. A fost un ajutor inestimabil pentru autoritățile federale, care erau în curs de a crea o formulă de spionaj



capabilă să-i ajute să identifice posibilele amenințări teroriste. În perioada care a urmat catastrofei, agenții FBI au studiat tranzacțiile cu cardurile de loialitate ale atacatorilor, în încercarea lor de a crea profiluri ale obiceiurilor de consumatori ale acestora.

O bună parte din arsenalul politicianului modern e exact pe identificarea grupurilor-țintă – exact ceea ce încearcă să facă cluburile de loialitate. Rapoarte recente, publicate în Marea Britanie și în Statele Unite, sugerează că transmiterea acestor date către terți se întâmplă mai des decât ar vrea cei din industria de retail să ne facă să credem. În Marea Britanie, Partidul Conservator a pus la punct „Trezorerii electorale”, în timp ce Partidul Laburist are baze de date similare, numite „Contacte laburiste”. Votanții sunt împărțiți în diferite grupuri diferențiate după criterii socio-economice, cum ar fi mașina pe care o conduc, codul poștal sau unde și de câte ori pleacă în vacanță. Informațiile permit partidelor să ne anticipeze intențiile de vot, ceea ce, mai departe, le ajută să se hotărască asupra mesajului pe care ni-l vor adresa. Contactul direct cu electoratul, prin intermediul e-mailurilor personalizate și al campaniilor telefonice, e o tehnică ce a fost rafinată, în Statele Unite, cu un succes uluitor de către directorul de campanie a lui George Bush, Karl Rove. Acesta a folosit 300.000 de voluntari într-o campanie de marketing multistratificată, utilizând informații precise pentru a se adresa votanților, circumscripție cu circumscripție. În timpul ultimelor trei zile ale campaniei, voluntarii pentru echipa Bush / Cheney au trimis e-mailuri la 7, 2 milioane de votanți. Multe dintre informațiile pe care le-au folosit proveneau din bazele de date ale cardurilor de fidelitate. O abordare similară a fost adoptată în 2005 de toate cele trei partide participante la alegerile generale din Marea Britanie.

Australianul Lynton Crosby, cel care l-a ajutat pe John Howard să adune patru victorii consecutive în Australia, a folosit sistemul Mozaic de clasificare, pus la punct de Experian (compania de evaluare a creditelor și de date ale consumatorilor) în timpul campaniei din 2005 a Partidului

Conservator. Sistemul împarte populația în 61 de categorii și 11 grupări. Lista votanților folosită de conservatori și laburiști se baza, în parte, pe referendumul din 2001 și, în parte, pe informații din sondajele în rândul consumatorilor și pe înregistrări ale cheltuielilor luate din bazele de date ale cardurilor de fidelitate.

Analistul de baze de date Joe Patel, care scrie pentru *Atlanta Constitution*, a afirmat că magazinele vând și folosesc ca monedă de schimb, în mod regulat, bazele de date care înregistrează preferințele clienților, compilate din mereu popularele carduri cu reduceri pentru cumpărături. *Media Week* a susținut că Tesco, Thomas Pink, MCV și New Look și-au scos, toate, la vânzare informațiile despre clienți, pentru alte companii de marketing.

Caspian Group, care militează împotriva sistemelor cu carduri de fidelitate, afirmă că datele culese de pe carduri sunt folosite, în mod regulat, în tribunalele britanice și americane. Detaliile despre vânzări pot fi stocate alături de imagini filmate ale posesorilor de carduri. Caspian susține că s-a înregistrat o creștere a cazurilor de cumpărători care au dat de bucluc din cauza unor greșeli făcute de analiștii care le-au studiat datele. Cu atâtea informații adunate și cu atâtea întrebuințări care se găsesc pentru ele în fiecare zi, astfel de probleme sunt inevitabile, iar abuzurile vor începe să se strecoare în sistem.

Deja există cazuri de analiști care au modificat programul ca să permită accesări ilegale. O femeie din Milton Keynes a fost arestată, iar casa i-a fost percheziționată de polițiști, după ce a fost filmată, pe un sistem de televiziune cu circuit închis dintr-un supermarket, în timp ce-și introducea în poșetă propria eșarfă. Paza magazinului a crezut că furase eșarfa și a identificat-o prin datele cardului ei de loialitate. Deși e foarte dificil, dacă nu chiar imposibil, să elimini toate riscurile unor asemenea incidente, care au legătură cu toate companiile cu care interacționezi, poți să îți micșorezi implicarea în programe acolo unde nu e obligatoriu să oferi informații personale. Și ține minte: chiar dacă folosești o identitate

„falsă” la supermarketul din zona ta, imediat ce scrii un cec sau folosești o carte de credit, ei pot pune în legătură acea informație cu profilul tău „fals”.

De fapt, nu datele sunt problema, ci oamenii pe mâinile cărora ajung ele. Avem de-a face cu o industrie care tolerează concepte precum „Wizmark” – un ecran de 8,5 cm, care e plasat în pisoare și activat de mișcarea lichidului. Curgerea declanșează un afișaj cu lumini pâlpâitoare, însoțite de un mesaj publicitar. Când e vorba de marketingul pentru industria de retail, orice e permis.

Riscul invadării intimității a crescut, în mod dramatic, odată cu introducerea identificării prin frecvențe radio (RFID) pentru o lungă listă de produse. Sistemul folosește cipuri minuscule de calculator, mai mici decât un grăunte de nisip, pentru a urmări mărfurile la distanță. Sunt cunoscute drept „cipuri-spion” și au fost ascunse în ambalajele multor produse – cum simt lamele de bărbierit Gillette – pe care le puteți cumpăra la supermarket. Fiecare cip e pus în legătură cu o antenă, care captează energia electromagnetică emisă de un dispozitiv de citire. Când detectează energia, cipul răspunde trimițând un număr de identificare unic lectorului, ceea ce permite identificarea obiectului. „Cipul-spion” poate transmite informații de la câțiva centimetri până la 30 de metri depărtare. Tehnologia e disponibilă din 1999 și toți marii comercianți din Marea Britanie au efectuat teste de fezabilitate pentru sistem. Dacă nu va apărea o rezistență organizată și zgomotoasă a consumatorilor, ei vor marca, în cele din urmă, fiecare obiect fabricat pe Pământ cu acest sistem, ca înlocuitor pentru codul de bare. Tesco, Procter and Gamble, Gillette și Wal-Mart au făcut, toți, experiențe în acest sens. Testele din Marea Britanie au fost, parțial, finanțate de Ministerul de Interne – un gest politic ce va fi, fără îndoială, scos din nou la iveală în viitor, când industria de retail va fi, în cele din urmă, trasă la răspundere.

În cel mai bun caz, tehnologia RFID ajută la urmărirea mărfurilor de la producător la depozit și apoi în magazin. Ar putea fi folosită la recuperarea unor comenzi pierdute sau la

alertarea echipei de securitate, atunci când un produs este furat. Într-un viitor nu prea îndepărtat, producătorii de bunuri pentru gospodărie ar putea veni din urmă creând, de exemplu, o tehnologie care să îți spună cum să prăjești o rață congelată pe care tocmai ai cumpărat-o sau cum să faci un sos gustos. Opoziția față de RFID se bazează pe protejarea intimității. Cu un cod de bare standard, nu produs precum o cutie de cola dietetică are un cod de produs universal, identic pentru toate cutiile de tipul respectiv. Dacă acest cod de bare ar fi înlocuit de RFID, fiecare cutie ar avea un număr de identitate unic. Acesta ar putea fi pus în legătură cu clientul care a cumpărat-o, respectivul putând fi identificat atunci când un card de credit sau de loialitate e scanat la teighea. Așadar, dacă mergi la Shopco și cumperi o sticlă de Head & Shoulders care e marcată cu RFID, plătind cu un cârd Visa și solicitându-ți punctele de pe un card de fidelitate, vei fi, iremediabil, pus în legătură cu acea sticlă de șampon (și cu faptul că ai mătreață). Comercianții aduc argumentul că raza de identificare a cipurilor e foarte scurtă. Acest fapt nu e adevărat, deoarece cipurile pot fi citite la distanță, cu un echipament mai sofisticat. Nu numai atât: ele pot fi, de asemenea, citite în portofelul sau în poșeta ta și prin haine, fără să ai habar de asta. Nu e nevoie decât de aparatul de citire potrivit. Ceea ce înseamnă că, atunci când ești pus în legătură cu un produs marcat, un străin poate să îndrepte un aparat de citire ascuns spre tine, pentru a afla conținutul genții sau al servietei pe care o porți și ce ai în buzunare, fără ca tu să-ți dai seama de nimic.

Când se va utiliza pe scară largă în Marea Britanie, tehnologia va permite sistemului să ne urmărească mișcările 24 de ore din 24. Dacă industria de retail va pune în aplicare ceea ce intenționează, vor exista cipuri și cititoare RFID pretutindeni. Ele vor fi ascunse sub dușumele, în avioane, magazine, frigidere și hoteluri. Nu numai că ne vom pierde intimitatea, dar vom fi bombardați permanent cu energie electromagnetică. Tehnologia a evoluat rapid și în prezent e posibil să „imprimi” cipurile-spion. Ceea ce înseamnă că un

punct de pe o pagină tipărită sau de pe o bucată de plastic poate fi folosit pentru a lua urma cuiva. Antenele pot fi, și ele, imprimate, făcând astfel cipurile-spion practic invizibile.

Tehnologiei, dezvoltate inițial în Japonia, i se minimizează în prezent importanța, comercianții susținând că e vorba de un simplu „cod de bare radio”. A fost adoptată ca o alternativă la codurile de bare normale, care nu sunt considerate sigure și care fac, tot mai des, obiectul unor escrocherii. Probabila trecere a comercianților la RFID a alarmat grupurile de presiune, care sunt conștiente că cipurile pot fi citite, de la mare depărtare, de dispozitive din afara magazinelor. Grupurile care luptă pentru drepturile cetățenilor și ale consumatorului au încercat să impună un boicot mondial, de exemplu împotriva magazinelor Shopco, deoarece ele au extins perioada de testare a sistemului. Protestatarii consideră că cipurile RFID ar trebui menținute în interiorul depozitului și al lanțului logistic, și nu ar trebui să li se permită contaminarea infospațiului cu poluanți care corodează intimitatea, dincolo de casele de marcat. Potrivit Grupului Caspian, RFID este prea rudimentar, din punct de vedere electronic, pentru a permite încorporarea unei tehnologii de criptare ce ar putea oferi niște garanții de protecție. Pentru a înrăutăți lucrurile, cipurile-spion nu pot fi „ucise” (anulate) la casa de marcat și, astfel, continuă să funcționeze la nesfârșit. Shopco și-a extins perioada de probă de 12 luni de la două magazine la zece și a comandat 4.000 de cititoare RFID și 16.000 de antene pentru incendii și de protecție de la compania ATD Security Services. Marks and Spencer a efectuat un test la șase dintre magazinele lanțului, în 2004. În timpul testului, clienții M & S nu au fost avertizați că achiziționează bunuri marcate.

Probabil singurele inconveniente ale cipurilor RFID vor fi costul și legislația. Tehnologia e costisitoare, menținându-se în prezent la puțin peste 15 penny bucata. Acest lucru adaugă un surplus destul de simțitor, să spunem, unei cutii de cola dietetică, și e foarte probabil ca prețul să rămână ridicat în viitorul apropiat. De asemenea, e posibil ca cipurile RFID să

contravină Legii protecției datelor din Marea Britanie și legislației europene cu privire la drepturile omului. E sigur că aceste sisteme vor fi puse la încercare la tribunal, atât în Statele Unite, cât și în Europa. În Germania, rețeaua de supermarketuri Metro a inclus RFID în sistemul lor de carduri de loialitate și și-a justificat gestul prin faptul că acest lucru le-a permis să verifice vârsta cumpărătorilor care doreau să vadă filmulețele promoționale ale unor DVD-uri pentru adulți. Informațiile despre cumpărător erau stocate într-o bază de date, conectată printr-o rețea wireless la un cititor RFID din secțiunea de DVD-uri a magazinului. În cele din urmă, Metro a abandonat testul, ca urmare a protestelor clienților. „Ne vom întoarce la codurile de bare”, au declarat ei. Totuși, au continuat prin a comenta că niciuna dintre celelalte zone în care Metro folosește tehnologia RFID nu va fi afectată de această decizie. „Suntem decizi să folosim RFID în managementul rețelei de aprovizionare”. Magazinul cere, în prezent, celor mai mulți dintre furnizorii săi să atașeze cipurile inteligente paletilor și ambalajelor de transport. Comerciantul american Target a impus o condiție similară furnizorilor săi locali, începând cu 2005. E doar o chestiune de timp până când sisteme asemănătoare vor fi folosite în Marea Britanie.

Tehnologia RFID se află încă la început, dar va deveni curând un lucru obișnuit în viețile noastre. Este acceptată, la scară foarte largă, în Statele Unite, unde e folosită în industria jocurilor de noroc. Acolo, tipurile sunt încastrate în jetoanele de joc, ca mijloc de a reduce fraudă și de a-i supraveghea pe marii jucători. Cazinourile britanice au examinat și ele sistemul, dar până acum au refuzat să-l întrebuințeze, invocând costurile și necesitatea sa redusă (ar fi ca și cum ai lua un baros pentru a sparge o nucă, au zis ei). Studenți de la universități din toată America sunt monitorizați prin intermediul cardurilor pe care le poartă, în care este inclus cipul. Când ajung la școală dimineța, RFID activează un ecran pentru a le înregistra sosirea și le afișează fotografia. Este eliminată astfel metoda manuală, mai veche, de a ține un

catalog de prezență. Astăzi, în loc să marcheze numele studenților pe o planșetă, sistemul este computerizat. Școlile și colegiile care îl folosesc spun că fac acest lucru pentru a implementa o securitate mai bună, un management al timpului ameliorat și o eficiență mai mare. Zece inspectorate școlare locale din Marea Britanie testează o idee similară. Este același sistem folosit pentru a-i urmări pe infractori englezi aflați în arest la domiciliu sau sub diverse interdicții de circulație, pe deținuții din penitenciarele din Texas și pe prizonierii irakieni de război. IBM a anunțat că intenționează să includă etichete electronice în cărțile de credit și în carnetele de cecuri.

După relaxarea reglementărilor de carantină antirabică pentru animalele din Europa, animalele pot fi inoculate, iar tratamentul poate fi înregistrat pe un cip electronic implantat în gâtul acestora. Multe mii de animale din Marea Britanie sunt marcate în acest fel, iar cipul îi ajută, de asemenea, pe angajații de la Protecția Animalelor să urmărească și să identifice exemplarele abandonate. Pentru americani a devenit un lucru obișnuit și, în unele locuri, la modă să aibă cipuri implantate în propriul corp. Companiile din Florida care utilizează tehnologia promovează deja această simplă operație cu argumentul că părinții și cei care au grijă de copii îi pot supraveghea astfel pe micuți. În 2004, o companie de securitate numită Metrorisk a implantat cipuri numite Verichips Procurorului General al Mexicului și altor zeci de colegi sau membri ai echipei sale. Cipul le permite accesul rapid în clădiri și săli de judecată protejate, fără a mai purta carduri de identitate. E adevărat că, atunci când vine vorba despre a ieși, într-un fel sau altul, în evidență, americanii au tendința de a fi mai puțin inhibați decât cetățenii altor țări, care ar putea să considere inacceptabilă implantarea unor cipuri de identitate în corpul lor, ca un procedeu ce permite economisirea de timp și de muncă. Tehnologia există și în Marea Britanie. Putem fi marcați, în mod discret, de chirurgii plasticieni de pe Harley Street. Totuși, aceasta tinde să fie o practică pe care englezii o țin secretă.

Utilizarea sistemelor de urmărire poate administra o lovitură mortală libertăților fundamentale. Grupul pentru drepturi cetățenești Liberty, cu sediul în Marea Britanie, susține că autoritatea asupra sistemului nu ar trebui lăsată companiilor comerciale, companiilor de securitate sau avocaților și contabililor particulari, atenționând că guvernul nu a elaborat încă niciun proiect de lege pentru reglementarea informațiilor generate de RFID. Tehnologia este foarte adaptabilă. Abonamentul folosit pentru metroul londonez o utilizează de peste doi ani. Cardul de transport are numele și adresa deținătorului și trimite informații ori de câte ori este scanat, la începutul și la sfârșitul călătoriei. Conform Autorității de Transport londoneze, datele vor fi păstrate „pentru o vreme”. Dacă îți plătești călătoria cu un card de credit sau de debit, așa cum fac multe persoane, traseele tale prin Londra vor fi înregistrate cu o precizie milimetrică. Toate mașinile britanice și europene au început să fie dotate cu dispozitive de urmărire începând din 2005 și poți cumpăra deja telefoane mobile cu astfel de dispozitive atașate. Banca Centrală Europeană a încorporat etichete electronice în toate bancnotele euro, iar Banca Americii studiază un cip produs de compania japoneză Hitachi, cu perspectiva de a marca bancnotele americane.

În urmă cu 30 de ani, pe lângă mai sus-amintita previziune despre puterea de procesare a computerelor, care se va dubla la fiecare 12 luni, fondatorul companiei Intel, Gordon Moore, a spus că orice dispozitiv sau sistem care folosește microcipuri va deveni rapid mai mic, mai mobil, mai eficient și mai puțin costisitor. Previziunea lui Moore se aplică, în egală măsură, internetului, care este construit din sisteme ce sparg datele în „pachete” sau în fragmente, le distribuie către destinațiile corecte și le reasamblează, la intervale de nanosecunde. Sistemul, cunoscut drept TCP/IP, a fost capabil să absoarbă o gamă largă de tehnologii pe lângă comunicațiile prin internet, inclusiv site-urile și serviciile de telefonie mobilă. Nu mai e mult până când telefoanele noastre, laptopurile, pagerele – de fapt, toate dispozitivele noastre de comunicare – își vor uni



forțele pentru a crea cel mai masiv sistem de supraveghere conceput vreodată. Zilele tranzacțiilor în numerar se apropie de sfârșit și fiecare achiziție va deveni un bit de informație înregistrat pe un hard disk și asociat, direct, cu detaliile personale ale individului implicat. Înregistrarea va dăinui până când discul va fi distrus.

Cardurile de fidelitate și dispozitivele de urmărire vor oferi întreprinderilor private mai multe informații personale despre bărbații și femeile de rând decât posedă, în clipa de față, cel mai tiranic dintre statele polițienești. Merită avantajele pe care le obținem din acest tip de săpare a datelor și din această tehnologie riscul pe care ni-l asumăm? Industria de retail și producătorii sistemelor RFID au susținut cu convingere că adunarea informațiilor despre tiparele de cumpărare este un procedeu demn de admirație, care aduce beneficii tuturor și care nu are nimic de-a face cu monitorizarea membrilor individuali ai publicului larg. Dar e sigur că vom putea să alegem să ieșim din sisteme care ne îngrijorează? Ce fel de protecție există pentru informațiile pe care aceste organizații le-au strâns în legătură cu noi? Acțiuni înregistrate pe cardurile de loialitate au fost deja folosite ca dovezi în tribunale. Puțini dintre noi îi abordează pe comercianți pentru a-și exprima îngrijorarea în legătură cu confidențialitatea și cu informațiile private pe care le adună despre noi. Tehnologia RFID va fi implementată, orice am face noi. Cardurile de loialitate au devenit o parte a vieții cotidiene. Singura metodă de a ne proteja pe care o avem la îndemână este să aruncăm cardurile de fidelitate și să plătim în numerar.

### Capitolul III

## Avem numărul dumneavoastră. Și numele...

*Obținerea rapidă și fără costuri suplimentare mari a unui credit a devenit un lucru obișnuit. Poți obține o ipotecă printr-o simplă convorbire telefonică. Nu va trebui să furnizezi prea multe date, numele și adresa vor fi de ajuns. După răspunsul la întrebarea dacă ești proprietarul apartamentului în care locuiești, vei primi un „Da” sau un „Nu” cât ai zice pește. În câteva secunde doar, poate fi vizualizat scoringul tău de credit, accesând una dintre cele 12 uriașe baze de date naționale aparținând unor companii precum Experian sau Equifax. Companiile de creditare și de ipotecare au contracte cu tot soiul de firme de acordare a scoringurilor și se folosesc de acestea fără prea mari muștrări de conștiință, pentru a-și forma o opinie pentru fiecare cerere primită. Problemele încep atunci când sistemul dă greș. Companiile de consultanță pentru acordarea creditelor sapă după informații financiare ale persoanelor, le includ în bazele lor de date, pe care apoi le vând. Aceste companii ajung să știe fiecare situație în care ai întârziat la plata unui împrumut. Sistemul nu este infailibil: datele pot proveni din surse îndoielnice, iar greșeli se pot face oricând. Corectarea acestor erori este, însă, o chestiune de noroc, pentru că aceia care acordă scoringuri nu vor niciodată să riște. Ei preferă să lase listele așa cum sunt și nu sunt dispuși să-și asume riscul de a gira un solicitant care să se dovedească apoi incapabil de a-și îndeplini obligațiile.*

Zeci de companii vând astfel de informații personale. Nicio instanță de creditare care se respectă nu își va furniza

serviciile cuiva înainte de a fi consultat una dintre multele agenții de acordare a scoringurilor, care a tot strâns astfel de informații despre tine de-a lungul întregii tale vieți ca adult. La urma urmei, banii acordați cu împrumut trebuie justificați în fața acționarilor sau a șefului. Simplificând, fiecărui adult îi corespunde un fișier cuprinzător, în care sunt înscrise toate elementele ce pot prezenta fie și o minimă relevanță în privința calității sale de potențial debitor. Informațiile incluse în fișier sunt cumpărate sau obținute din arhive publice – precum cele ale tribunalelor, ale Protecției Sociale sau ale Oficiului de Cadastru – ori private (neachitarea la timp a obligațiilor ce privesc cărțile de credit, creditele bancare sau leasingurile). Profilul persoanei este înscris într-o bază de date, iar apoi pus la dispoziția abonaților sau a oricui are nevoie de aceste informații și este dispus să plătească pentru ele.

Scoringurile sunt utilizate de poliție și de serviciile secrete pentru a construi profiluri ale persoanelor implicate în investigațiile în derulare. Unele date sunt mai prețioase decât altele. Se poate dovedi dificilă inițiativa de a achiziționa informații privind o persoană sau un grup care posedă un statut aparte. În Marea Britanie, conform Legii protecției datelor, dosarul personal trebuie arătat, la cerere, subiectului său. Și totuși, chiar și în acest caz, companiilor li se permite să perceapă un tarif pentru că-ți trimit elemente din propriul dosar.

Experian este una din cele mai mari companii britanice de acordare a scoringurilor. Compania poate informa un potențial creditor dacă un solicitant a declarat vreodată faliment, dacă a fost nevoit să cadă la înțelegere cu alți creditori, dacă a scris vreodată cecuri neacoperite, dacă a sărit o rată, de orice fel ar fi aceasta, sau dacă a fost cândva condamnat pentru fraudă. Când și când, poate oferi alt tip de informație utilă creditorilor, precum numărul de înregistrare la Protecția Socială sau numărul de înmatriculare al mașinii, de câte ori solicitantul a încălcat Codul Rutier sau dacă și-a schimbat cu regularitate furnizorul de cărți de credit, pentru a

beneficia de o dobândă mai bună. Banca sau furnizorul de credit abonat plătește pentru datele primite și are tendința să le trateze ca literă de lege. Acordarea creditelor este o afacere de amploare și cei care dau bani cu împrumut nu sunt foarte flexibili în ceea ce fac. Nu există excepții de la regulă.

Datele de eligibilitate la solicitarea creditelor nu reprezintă singurul gen de informație disponibilă pe piață. Profilurile psihologice ale angajaților sunt cumpărate în mod curent de către agențiile de recrutare și de către instituțiile publice, inclusiv de cele de învățământ sau de menținere a ordinii publice. În Marea Britanie, unde „pedofilul răpitor” a devenit sperietoarea publică cu cea mai mare vizibilitate, reguli foarte restrictive stabilesc cine este și cine nu este potrivit pentru a lucra cu copii. Tuturor profesorilor și angajaților din învățământ li se verifică minuțios trecutul profesional, precum și alte înregistrări despre ei, înainte de a li se permite să înceapă lucrul. Chiar și jucătorii de golf profesioniști, instructorii de înot sau de cercetăși trebuie să aibă dosare ireproșabile pentru a li se permite să-i învețe pe copii. Iar responsabilitatea de a se asigura că toți membrii personalului sunt dincolo de orice suspiciune, înainte ca aceștia să înceapă lucrul, le revine angajatorilor.

Furnizorilor de date li se cere în mod frecvent să ofere informații de bază. Dacă ele sunt eronate, îi pot stigmatiza pe cei la care se referă. Dacă persoana care a fost nedreptățită dorește să se adreseze justiției, unica sa opțiune este de a recurge la legile civile ale defăimării – pentru care, în Marea Britanie, rareori se poate oferi consiliere juridică. El sau ea ar mai putea invoca Legea drepturilor omului sau s-ar putea adresa Curții Europene, dar, indiferent unde ar căuta reparație legală, are în față un proces lung și care îi va pune serios nervii la încercare. În Statele Unite există legi care le protejează pe victimele informațiilor inexacte. Cea mai importantă este Legea raportării corecte a datelor necesare obținerii creditelor (1970), care reglementează accesul la date și dreptul de a corecta inexactitățile. Și cam atât.

Din păcate, agențiile de acordare a scoringului și alte

companii care manevrează informații de ordin personal sunt recunoscute pentru obiceiul lor de a furniza date inexacte. Pentru aceasta pot exista două motive: fie au primit, la rândul lor, informații incorecte, fie aceste informații sunt corecte, dar au fost introduse greșit în baza de date. Deși Legea protecției și Legea libertății informațiilor din Marea Britanie garantează accesul la date, acestea nu asigură în același timp și aducerea la zi sau corectarea în timp util a bazelor de date, atunci când se descoperă inadvertențe. În industria informațiilor nerespectarea drepturilor cetățenești frizează aroganța. Situațiile în care mai multe persoane au descoperit că fuseseră clasificate, în mod eronat, ca fiind necinstite sau că înregistrările privind activitățile și caracterul lor fuseseră alocate altei persoane ori erau pur și simplu răuvoitoare sunt deja banale.

Multe persoane vârstnice sunt puse în situații jenante de agențiile de obținere a informațiilor financiare. Companiile furnizoare de cărți de credit refuză adesea efectuarea tranzacțiilor, fie și din motivul că utilizatorul nu și-a folosit cardul de ceva vreme. În momentul achitării cumpărăturilor, furnizarea de lichidități este refuzată automat, cu toate neplăcerile ce decurg din aceasta. Există multe situații în care coeficientul cuiva poate avea de suferit din cauze neimputabile lui. Exemplul tipic este acela al diferendului legal dintre bancă și client pe marginea unui împrumut neachitat. Clientul poate crede cu tărie că are dreptate. În mod cu totul arbitrar, banca decide să lase rezolvarea disputei pe mâinile unei agenții de recuperare a debitelor și să paseze informațiile unor companii precum Experian sau Equifax. Clientul poate să meargă până în pânzele albe cu contestarea datoriei, astfel încât primii recuperatori de debite pot vinde „datoria” acestuia altei firme, încă și mai lipsite de scrupule. Așa-zisul debitor, sătul, în cele din urmă, de această neîntreruptă hărțuire și dorind pur și simplu să rezolve până la urmă problema, decide să plătească acestui al doilea recuperator. Chiar și așa, banca clientului a înregistrat acum împrumutul și refuză ștergerea din evidențe a întârzierii plății,

pe motiv că nu deține nicio dovadă că aceasta a fost în cele din urmă efectuată. Întârzierea este deja irevocabilă și va influența pe vecie scoringul debitorului. Asemenea datorii sunt vândute în mod obișnuit unor terțe companii financiare.

Comerțul cu informații transcende granițele țării, iar cele mai mari companii din branșă (Equifax, Lexisnexus și Choicepoint) operează în întreaga lume. Ele sunt cunoscute ca brokeri de informații comerciale și reprezintă afaceri uriașe, care utilizează tehnici avansate, având milioane de abonați și miliarde de nume înscrise în bazele lor de date. De asemenea, aceste companii achiziționează informații din bazele de date ale altor țări. Caracterul informațiilor personale deținute de ele nu se rezumă la relevanță în cazul acordării unui credit și nici la furnizarea de referințe angajatorilor. Informațiile lor nu sunt vândute doar în domeniul industriei și comerțului, ci și agențiilor guvernamentale și poliției.

Lexisnexus a admis recent posibilitatea ca datele personale ale 310.000 de cetățeni americani să fi fost furate în timpul unei căderi a sistemului de securitate, la începutul lui 2005. Când au fost pentru întâia oară interpelați pe marginea acestui incident, reprezentanții companiei au declarat că disfuncțiile sistemului de securitate au afectat doar câteva dintre numeroasele lor baze de date, conținând detalii a doar 32.000 de persoane – cam 10% din numărul real. Lexisnexus a adăugat că penetrarea ilegală a bazelor de date, prin intermediul parolelor furate, a avut loc de cel puțin 59 de ori, ceea ce a mijlocit accesul hackerilor la adrese, la numere de Protecția Socială, precum și la alte date importante. Aceasta este numai ultima dintr-o lungă și de succes serie de încercări de a fura informații personale de identificare, care a afectat sute de mii de cetățeni din America de Nord și Europa.

În cursul depozităților în fața Congresului, grupuri de militanți pentru protejarea intimității și a drepturilor cetățenești, precum EPIC (Centrul pentru Intimitatea Datelor Electronice), au solicitat înăsprirea legislației privind brokerajul de date, utilizând drept argumente lipsa transparenței și a unei evidențe clare. Plângerile împotriva

Experian și a altor agenții de scoring au fost nu puține și de toate felurile. Intimitatea a devenit o chestiune sensibilă într-o lume în care tot ceea ce facem este înregistrat și trecut într-o bază de date, iar normarea strictă a industriei de informații reprezintă o inițiativă care întârzie de ani buni. Consumerfiifo.com, subsidiară-fumizor de informații pentru companii precum Experian, Equifax și Transunion, a fost acuzată de a fi încălcat legile Statelor Unite atunci când a făcut reclamă calculării „gratuite” a scoringului propriu, care, odată făcută comanda, angaja clientul într-o relație de tip abonament, pe termen lung și cu costuri ridicate, fără a-l înștiința în privința condițiilor contractului (inclusiv a posibilităților de reziliere). Compania a fost acuzată, de asemenea, că și-a sporit veniturile prin suscitarea de temeri în legătură cu acuratețea scoringurilor, și provocând un val de cereri de vizualizare a rapoartelor prin intermediul propriului site.

Procesul împotriva Consumerfiifo.com a fost intentat de EPIC, care a atras atenția asupra absurdității situației în care o agenție de scoring face reclamă unei subsidiare, prin care clientul plătește pentru a verifica societatea-mamă, precum și alte firme cărora aceasta le-a vândut informații. EPIC a folosit oportunitatea ca pe o modalitate de a solicita o legislație strictă a tuturor agențiilor de scoring, forțându-le să ofere posibilitatea de a-și vizualiza gratuit propriul raport. Pentru acest serviciu, în Marea Britanie se percepe o taxă de trei lire sterline. Mesajul publicitar al Consumerinfo.com evidențiază faptul că undeva, în industria marketingului de date, se prea poate să existe o companie care vehiculează informații greșite despre tine. Problema rezidă în faptul că acea companie ar putea fi chiar cea care își face reclamă. Iată-l pe Kafka, în toată splendoarea sa.

Însă se poate și mai rău. Când consumatorii sunt de acord să colaboreze cu un serviciu de monitorizare a scoringului pe bază de abonament, li se cer informații personale pentru a le fi validată identitatea. Creditorul are dreptul de a transmite mai departe aceste informații tuturor abonaților firmelor

afiliate la agenție. Consecința este că majoritatea persoanelor care doresc să-și protejeze intimitatea renunță, fără să-și dea seama, cu totul la ea. Asta înseamnă că utilizatorii care doresc să se aboneze la agențiile de scoring, pentru a avea cât de cât control asupra informațiilor ce îi privesc și pentru a-și proteja propria intimitate și corectitudinea datelor, obțin în realitate tocmai contrariul. Practicile de marketing ale agențiilor de scoring, bazate pe exploatarea temerilor consumatorilor privind caracterul posibil eronat al rapoartelor, sunt, fără dubiu, îndoielnice din punct de vedere moral.

Simon Davies, directorul sucursalei britanice a Privacy International, este specialist în dezvoltarea companiilor care vehiculează informații personale și are o experiență îndelungată în problemele ce apar în acest domeniu. Privacy Internațional și grupul asociat EPIC au fost implicate în mai multe confruntări cu firme precum Choicepoint, a căror creștere, mai ales după 11 septembrie 2001, a fost spectaculoasă.

Choicepoint, cu sediul în Georgia, Statele Unite, vinde informații către, printre alții – asigurători, agenții guvernamentale și industria marketingului. Conform raportului său trimestrial, înaintat Comisiei pentru Securitate și Schimb, Choicepoint vinde „solicitări de despăgubiri, rapoarte privind autoturismele deținute, arhive ale poliției, informații privind creditele și calculul probabilităților îndeplinirii angajamentelor financiare ulterioare, (...) experiențe profesionale și rezultate ale controalelor antidoping, rezultate ale căutărilor în arhivele publice, date de stare civilă, servicii de verificare a veridicității titlurilor și calităților oficiale deținute, rapoarte de audit legal și contabil, date din Registrul Comerțului, servicii de identificare după ADN, servicii de autentificare și de localizare a persoanelor și acționarilor, (...) listare, servicii de call center și de administrare a bazelor de date și a unei campanii (...)”.

De când s-a desprins de Equifax, în 1997, compania a acumulat un procent semnificativ din piața brokerajului de informații comerciale, prin preluarea a 38 de alte firme



similare, fiind în prezent unul dintre cei mai importanți jucători din domeniu. Aceste achiziții includ nume precum Pinkertons inc, National Data Retriever inc, CITI Network, Bode Technology și Accident Report Services, printre multe altele. Conform *Wall Street Journal*, Choicepoint a furnizat recent informații personale unui număr de cel puțin 35 de agenții guvernamentale, compania având în același timp în derulare contracte cu grupuri de impunere a legii în valoare de mai multe milioane de dolari.

Printre informațiile tranzacționate de Choicepoint se numără și cele de identificare cu care începe un raport de scoring. Adică numele și adresa persoanei, numele soției, adresa anterioară, numărul de telefon, numărul de la Protecția Socială și angajatorul curent. Compania mai pune la dispoziția abonaților serviciul numit „etalon preangajare”, care cuprinde rapoarte financiare, verificare de diplome și scrisori de recomandare, cazier (dacă există), încălcări ale Codului Rutier, verificare a datelor de la Protecția Socială. O altă facilități e dată de așa-numita „estimare a bunurilor”, care se referă la averea pe care o deține o persoană. Choicepoint mai oferă posibilitatea contractării căutărilor cu probabilitate redusă, ceea ce, în doar câteva minute, înlesnește agențiilor de păstrare a ordinii publice accesul la profilul complet al unei persoane, având drept punct de pornire un simplu prenume sau o adresă parțială. Aplicația în cauză se numește Smartsearch. Introducând în baza de date toate detaliile cunoscute despre o persoană, cum ar fi numele, vârsta, orașul sau regiunea de reședință probabile, programul poate indica unica persoană care întrunește toate aceste criterii, afișând totodată adresa actuală a acesteia. Însă Choicepoint nu deține doar o listă a adreselor rezidențiale, ci și una cu personalul militar american și britanic ori cu deținătorii de aparate de zbor și de ambarcațiuni, pentru a facilita localizarea unei persoane.

Unul dintre produsele cele mai populare ale Choicepoint este aplicația complexă AutotrackXP, care permite atașarea unei cantități semnificativ mai mari de informație la fișa unei

persoane, prin intermediul așa-numitelor „servicii de asociere”. Acestea descoperă numeroase conexiuni între subiect și alte date personale obținute la nivel național, provenind, de pildă, de la clienți și birourile de taxe și impozite. AutotrackXP poate, de exemplu, să creeze legături între adresele anterioare ale unei persoane și numele tuturor celor care au indicat aceeași adresă în documente precum carnetul de conducere.

Detaliile adiționale includ permisele de tot felul aflate în posesia unui subiect, cum ar fi cele de conducere, de pilotaj sau de deținere a unei arme de foc. De asemenea, elemente incluse în cartea de muncă, informații privind afacerile persoanei, scrisori de recomandare, calificări și adeziuni, bunuri deținute, bunuri tranzacționate sau cedate, actele aferente deținerii sau conducerii unui vehicul, a unei bărci sau a unui aparat de zbor, numărul de Protecție Socială, precum și orice informații din arhive publice, cum ar fi arestări, acuzații, sentințe legale ori falimente. Acest produs mai furnizează liste telefonice complete și servicii de individualizare a unui abonat după numărul de telefon utilizat.

Choicepoint a dezvoltat o tehnică numită „căutarea Soundex”, bazată mai degrabă pe modul în care un nume este rostit decât pe felul în care este el scris. Mai mult, informațiile oferite îi pot viza pe vecini sau pe membrii familiei unui suspect. De fapt, Soundex va construi un profil complet, conținând informații contextuale privind mediul social căruia îi aparține subiectul, cum își petrece el timpul liber, cum ajunge la serviciu, de unde își face cumpărăturile zilnice și unde merge cu mașina.

Ca o organizație de asemenea dimensiuni, care are drept obiect de activitate obținerea și diseminarea unei cantități uriașe de informații personale, ar trebui să fie normată la sânge, este o ipoteză de bun-simț. Și totuși, multe dintre produsele oferite nu se supun legislației americane în vigoare. Unele produse de „dosar personal”, precum raportul AutotrackXP al Choicepoint, sunt vândute fără ca respectarea

US Fair Credit Reporting Act, lege americană care reglementează în linii generale, colectarea, distribuirea și utilizarea informațiilor cu privire la creditele de consum, să fie obligatorie.

Comisia Federală pentru Comerț (FTC – Federal Trade Commission) investighează în prezent activitatea Choicepoint și a altor brokeri de informații. Ancheta a fost lansată, în parte, ca urmare a unei plângeri înaintate de organizațiile de respectare a drepturilor cetățenești, în decembrie 2004. Aceste organizații au solicitat o investigație a „produselor tip dosar personal” oferite de brokerii de informații, printre care Choicepoint. Cei de la EPIC sunt de părere că asemenea servicii constituie „rapoarte de consumator” și se supun prevederilor Fair Credit Reporting Act.

Astfel stând lucrurile, atât furnizorul, cât și clientul său se supun, la rândul lor, prevederilor actului menționat. O chestiune intens dezbătută a fost dacă firmele ori agențiile de detectivi particulari sau forțele polițienești sunt îndreptățite să aibă acces la datele vehiculate fără știința ori permisiunea persoanei la care se referă. EPIC – și nu numai – consideră că transmiterea către poliție a datelor personale furnizate de către o persoană în scopul primirii unui credit, fără știrea acesteia, reprezintă un abuz. Cei mai mulți consumatori sunt, fără îndoială, împotriva ideii de transmitere a informațiilor personale pentru a servi unui scop diferit de cel pentru care ele au fost raportate inițial. Deși, în Marea Britanie, Legea protecției informațiilor este menită să rezolve această dilemă, rareori s-a ajuns ca ea să fie invocată în sălile de judecată.

Rapoartele AutotrackXP sunt similare ca scop și utilizare scoringurilor standard, protejate de către lege. EPIC susține că, prin vânzarea datelor personale fără respectarea prevederilor actului menționat, Choicepoint eludează scopul pentru care a fost instituită această lege federală privind restricționarea informațiilor cu caracter privat. Conform EPIC, companiile precum Choicepoint și produsele ca AutotrackXP țin de o epocă apusă, aceea în care legislația de protejare a subiecților companiilor de recoltare a datelor încă nu fusese

implementată. În trecut, asemenea firme nu trebuiau să dea socoteală nimănui și vehiculau adesea informații inexacte, falsificate ori irelevante despre persoane fizice. Uneori, într-o industrie de amploarea celei a colectării informațiilor, profilurile puteau fi falsificate deliberat, pentru a crește în mod artificial prețul asigurărilor sau al creditelor. Efectul era trecerea subiecților, în mod nejustificat, pe o listă neagră a persoanelor cu grad ridicat de risc, astfel încât ei erau puși în situația de a plăti mai mult furnizorului de credit sau de asigurare (în general companii mai puțin respectabile). După cum era de așteptat, Choicepoint a respins aceste acuzații și a suscitât o dezbatere națională pe marginea acestui subiect.

Și alte probleme puse în discuție de către militanții americani pentru dreptul la intimitate sunt semnificative în chestiunea creșterii anvergurii brokerilor de date personale. O asemenea problemă o ridică un articol publicat în *Washington Post*, în care compania Choicepoint este acuzată că se comportă precum un serviciu secret, concluzia fiind că este necesar ca industria obținerii informațiilor să se supună unei noi legislații, dat fiind modul de utilizare a datelor personale. Articolul face referire la uriașul capital de încredere câștigat de brokeri în privința informațiilor ce pot fi folosite în investigații oficiale. După 9/11, ponderea utilizării datelor personale a crescut exponențial în Statele Unite și Marea Britanie. Este, de bună seamă, de importanță vitală ca informațiile folosite în scopul creării giganticele baze de date antiterorism, precum CAPPSII, să fie reale și ca practicile neguțătorilor de date să fie perfect transparente. Choicepoint se bucură de aproximativ 100.000 de clienți, printre care 7.000 de agenții de impunere a legii. Cifrele nu includ clienții din Marea Britanie ori Europa.

Dovezile înaintate Comisiei Federale pentru Comerț de către EPIC includ o copie a listei de mailing a Politechbot.com. Un detectiv particular, utilizator al Choicepoint, susține că firma incriminată arhivează rapoartele de audit ale clienților care au avut acces la informații cu caracter personal. Dovada furnizată de EPIC este utilă,

deoarece instanțele de păstrare a ordinii publice nu pot fi auditate și nu a existat niciodată o situație în care un broker de informații să dea un utilizator pe mâna justiției, ca urmare a dovezilor furnizate de un astfel de audit, conform căruia acel utilizator a abuzat de serviciile furnizate.

EPIC a înaintat, de asemenea, copia unui documentar de televiziune intitulat *Cineva te urmărește*, difuzat pe 18 decembrie 2004 de Discovery Times Channel și care s-a bucurat de o largă audiență în Statele Unite. În film, doi investigatori particulari demonstrează cât de simplu poate fi ca, prin intermediul unei agenții de date, să obții accesul la numărul de Protecție Socială al unui străin, la date privind traiectul profesional al acestuia ori la alte informații, și asta fără ca niciun fel de justificare legală să fie necesară.

Apoi, în februarie 2005, industria protecției informațiilor a fost zguduită de una din cele mai uimitoare declarații făcute vreodată. Compania Choicepoint a fost obligată să anunțe că a vândut informațiile personale a cel puțin 145.000 de cetățeni americani, majoritatea din California, unei rețele infracționale specializate în furtul de identitate. Poliția din California a raportat, între timp, utilizarea de către infractorii-clienți ai Choicepoint a materialului achiziționat în schimbarea neautorizată a adreselor a cel puțin 750 de persoane, iar anchetatorii sunt de părere că au fost compromise informații personale a până la 400.000 de persoane din întreaga țară. Organizațiile de militanți pentru respectarea drepturilor cetățenești au fost scandalizate și au cerut companiei să îi înștiințeze pe cei ale căror informații au fost transmise membrilor rețelei în ceea ce privește natura și conținutul datelor în cauză. Nu doar din rațiuni de corectitudine și dreptate, susțin aceștia, ci și pentru a răspunde temerilor generale privind siguranța publică.

Apoi, în martie 2005, în cadrul unei audieri în fața Comitetului Senatorial pentru Bănci din California, companiile de administrare a informațiilor, cum sunt Choicepoint, Lexisnexis și Acxiom, au fost aspru criticate de senatoarea Jackie Speier, președinta comitetului. Ea a dorit să afle cum

au putut sistemele Choicepoint să fie înșelate cu atâta ușurință de către un grup de infractori cu un nivel rudimentar de pregătire, precum și din ce motiv compania nu a raportat scurgerea de informații de îndată ce aceasta a fost descoperită. În replică, Choicepoint și-a cerut scuze pentru faptul de a fi vândut informații unor infractori și a afirmat că va „sista vânzarea de produse informaționale conținând date personale sensibile”, incluzând aici numerele de Protecție Socială și de înmatriculare a autovehiculelor, „cu excepția cazurilor când este vorba de un beneficiu sau o tranzacție orientate către consumator” sau când produsele „sunt utilizate în interesul structurilor federale, statale sau locale ori cazuri penale”.

Multora, acesta li se va fi părut un răspuns prea prudent, având în vedere consecințele scurgerii de informații. Compania a declarat că firmele mici vor putea în continuare achiziționa rapoarte personale, însă se pare că numerele de Protecție Socială nu vor mai figura în ofertă. De asemenea, Choicepoint a anunțat că lucrează la un sistem care să ofere acces la produsele sale informaționale. Însă persoanele particulare nu vor putea să își corecteze înregistrările provenind din arhivele publice, nici măcar în situațiile în care acestea au fost redactate eronat. Cu toate acestea, numărul de Protecție Socială va fi eliminat automat din aceste înregistrări.

În timpul audierii din California, directorul comitetului a cerut brokerilor de informații clarificări în privința propriilor definiții a ceea ce reprezintă date „sensibile”, precum și dacă termenul include numerele de Protecție Socială sau de înmatriculare a autovehiculelor. Când acestea apar în arhivele publice, Lexisnexis, de pildă, nu le consideră ca fiind sensibile și le vinde fără cea mai mică ezitare. Senatorul Speier a declarat că este de părere că, în ochii multor oameni, aceste detalii sunt „cu adevărat cât se poate de sensibile”, adăugând că „noțiunea de «sensibil» a brokerilor de informații nu pare să reflecte realitatea”.

Choicepoint a folosit în reclamele sale frica drept mijloc de a-și promova serviciile, susținând, de exemplu, că previne agresiunile pedofililor asupra copiilor și că bazele sale de date

au ajutat la găsirea multor copii dispăruți. Senatorul Speier i-a întrebat pe cei de la Choicepoint cât din procentul activității lor reprezintă localizarea acestor copii dispăruți, întrebare rămasă fără răspuns.

EPIC nu numai că a condamnat direct reformele propuse de Choicepoint, considerându-le „inadecvate”, dar a și subliniat faptul că ele nu rezolvă protejarea datelor private în brokerajul de informații comerciale. Mai cu seamă, aceste schimbări nu obligă și firmele rivale, astfel încât alți brokeri de date pot continua nestingheriți să vândă detalii precum numărul de Protecție Socială oricui găsesc de cuviință.

EPIC a adăugat că „nici măruntele schimbări de procedură [proapse de Choicepoint], nici revelarea faptului că au existat o serie de scurgeri de informații la mai multe bănci și universități importante nu au adus atingeri majore unei piețe dubioase complexe, a vânzării și revânzării de informații personale, în continuare vulnerabile în fața unor fraude similare”.

Se pare că Choicepoint are de gând să tranzacționeze în continuare rapoartele din arhive publice, aflate în afara reglementărilor, către firmele mici, de data aceasta cu numerele de Protecție Socială și de înmatriculare a autovehiculelor „trunchiate”, adică prescurtate. Însă marile companii și forțele polițienești vor putea obține în continuare rapoarte complete, conținând toate „informațiile sensibile” posibile. Încă nu se știe cu precizie cum va fi „trunchiat” numărul de Protecție Socială. Există voci care susțin că va fi posibil ca firmele mici – și nu numai ele – să folosească sistemul în sens invers, obținând astfel numărul întreg. O soluție ideală ar fi, fără îndoială, eliminarea cu totul a acestui număr din rapoarte, mai degrabă decât „trunchierea” sa, la care există riscul de a putea fi depistat numărul original prin compilarea diferitelor surse.

Conform unui raport al Forumului Mondial pentru Intimitate, rapoartele de informații publice ale Choicepoint au o „rată ridicată de eroare”. În etalonul propus, 90% din rapoartele obținute conțineau greșeli, multe din acestea grave,

iar altele de-a dreptul ridicole, cum ar fi indicarea altui sex în dreptul unor persoane. Constatările inițiale ale analistului Forumului, Pam Dixon, sunt susținute și de relatările alarmante ale altor persoane care și-au citit propriile rapoarte Choicepoint, din care au fost excluse informațiile reglementate. După parcurgerea propriului dosar, cercetătorul Richard Smith a declarat că acesta „conținea mai multe neadevăruri decât informații corecte”. Elizabeth Rosen, infirmieră cu domiciliul în California și una din multele victime ale scurgerii de informații Choicepoint, a descoperit că din șase pagini, câte avea dosarul său, cinci conțineau erori. De pildă, raportul o indica în mod greșit drept funcționară în Texas, având o casuță poștală privată la *Mailboxes Etc.* Și deținând, printre mai multe afaceri, un magazin de delicatese numit Zach's. Doamna Rosen a amintit, în cadrul anchetei, despre frustrarea ei atunci când compania a refuzat, inițial, să-i prezinte dosarul complet și despre multele demersuri care s-au dovedit a fi necesare pentru a obține datele în cauză. Întrebat de ce compania sa a refuzat să înmâneze un raport solicitat persoanei la care se referea, reprezentantul Choicepoint nu a putut oferi un răspuns.

Choicepoint afirmă acum că în viitor oamenii vor putea avea acces la rapoartele conținând informații publice care nu se supun legilor în vigoare, dar nu vor avea dreptul de a corecta acele informații. Motivul invocat de Choicepoint este acela că informațiile nu pot fi corectate, dat fiind că ele provin din arhive publice. Însă s-a dovedit deja, în repetate rânduri, că Choicepoint a încurcat informații referitoare la indivizi diferiți. Astfel, Deborah Pierce, care a reușit să-și obțină „dosarul național complet” de la Choicepoint, a descoperit cu stupeoare din el că ar putea avea cazier în Texas. Că o persoană din baza de date a Choicepoint are cazier în Texas se prea poate să fie adevărat, dar acea persoană nu este cu siguranță Deborah Pierce.

Potrivit lui Simon Davies de la Privacy International din Londra, nimic nu poate obliga Choicepoint să își respecte promisiunile de a-și și menține practicile nou-implementate.



În ultimii ani, s-a dovedit că mai multe companii mari, printre care ebay.com, Amazon.com, drkoop.com și yahoo.com, au modificat setările de siguranță ale utilizatorilor sau au schimbat propriile politici de limitare a accesului la informații personale în detrimentul utilizatorilor. Din punct de vedere legal, Choicepoint se află într-o poziție favorabilă încălcării propriilor angajamente, dat fiind că nu recunoaște existența unei legături directe cu consumatorii, care ar putea servi drept pretext pentru o acțiune în instanță. Pentru Choicepoint, „consumatorii” sunt companiile care achiziționează informații, nu persoanele la care se referă acele informații. Protecția Socială Choicepoint a emis un comunicat de presă în care a anunțat că își rezervă dreptul de a tranzacționa informații personale „sensibile” către persoane juridice pe mai multe căi. Astfel, datele sensibile vor fi vândute „pentru a asista la efectuarea tranzacțiilor orientate către client, atunci când sunt necesare unele informații pentru a consfinți sau menține o relație de afaceri, (...) pentru a oferi instrumente de autentificare și prevenire a infracțiunilor vizând mari corporații, cu care consumatorii au deja relații, (...) pentru a ajuta guvernele federale și statale, administrațiile locale, polițiile și agențiile de informații în îndeplinirea misiunilor lor importante”. Ce reprezintă oare exact „tranzacții orientate către client”? Și când este nevoie de informații „pentru a consfinți sau menține o relație de afaceri”? Această declarație nu este altceva decât o bâlbâială a unui PR-ist năucit, care se trezește din senin că trebuie să înfrunte focul încrucișat al întrebărilor reprezentanților mass-mediei.

Choicepoint se află în poziția fericită de a putea decide pe cont propriu ce anume reprezintă „beneficiul consumatorului”, în trecut, compania a avut o încercare de a furniza propria definiție a acestui termen, susținând că se va împotrivi demersurilor de a șterge orice fel de informație din bazele de date deținute, deoarece „considerăm că ștergerea informațiilor ar reduce utilitatea acestor produse pentru afaceri, ceea ce ar fi, în cele din urmă, tot în detrimentul consumatorilor. Ce crede Choicepoint că e bine pentru

consumatori nu e însă și ceea ce consumatorii cred că e bine pentru ei înșiși.

Politica Choicepoint îi permite companiei să vândă dosare complete, în scopul prevenirii fraudelor. Inițiativă teoretic laudabilă și de bun-simț, însă, practic, aproape orice tranzacție reprezintă o potențială fraudă. Dacă se optează pentru păstrarea acestei politici, ea îi va permite companiei să continue să vândă informații personale, chiar și atunci când riscul de fraudare este minim ori este utilizat drept pretext pentru colectarea în alt scop a informațiilor.

În cursul audierilor din California, Choicepoint a ridicat un pic cortina, dezvăluind structura principalului său obiect de activitate: un procent de 5% din afacere e reprezentat de „distribuția informațiilor către polițiile locale și federale, pentru a înlesni investigațiile în curs”, iar 6% – de „ajutorul acordat cabinetelor de avocatură, instituțiilor financiare și altor organizații, în scopul reducerii riscurilor prin informații și autentificare de date, inclusiv suport juridic ori de date necesare recuperării datoriilor”. Un alt procent de 20% îl reprezintă vânzarea de software și tehnologie fără legătură cu distribuirea de informații personale.

În dezbaterile legate de propriile strategii, Choicepoint nu specifică întotdeauna dacă se referă la rapoartele reglementate sau nereglementate legal, producând confuzie atât în rândul publicului, cât și printre legiuitori. Aproximativ 60% din afacere îl reprezintă „tranzacțiile inițiate de către consumator”, cele mai multe reglementate de Fair Credit Reporting Act, legea ce reglementează utilizarea informațiilor necesare pentru credite. Astfel de tranzacții includ eșantionarea preangajare și servicii de evaluare a preasigurării, estimarea riscurilor unui potențial chiriaș, oferirea de informații de maximă importanță utilizatorilor, întocmirea de asigurări împotriva daunelor. Aproape 9% din afacere sunt serviciile de marketing, care nu implică distribuția de date personale, dar care se supun reglementărilor statale și federale ce interzic trimiterea nesolicitată, telefonic sau prin e-mail, a informațiilor către

public.

Faptul că propunerile de „reformă” ale Choicepoint nu limitează vânzarea de informații personale către poliții – fie ele federale, locale sau statale –, către poliția britanică sau către departamentele de finanțe sau de imigrare, ar trebui să reprezinte un semnal de alarmă pentru oricine intră în vizorul companiei. Grupurile americane de militanți pentru drepturile cetățenești susțin că legiuitorii ar trebui să trateze problema traficului cu date personale nu ca pe o chestiune de securitate, ci ca pe un atentat la viața privată. Chiar și atunci când informațiile personale sunt utilizate securizat, rămâne problema tranzacționării lor către o paletă largă de organizații, persoanele implicate neavând niciun cuvânt de spus în această privință.

Cam acesta este viitorul pieței informaționale. Cererea de date personale crește în America, în Marea Britanie și în restul Europei. Piese-le-lipsă sunt regulamentele și legislația aferente. Suntem permanent monitorizați, iar ceea ce este înregistrat se vinde. Când vom începe, în cele din urmă, să ne exprimăm temerile privind pierderea dreptului nostru la viață privată, s-ar putea să fie deja prea târziu.

## Capitolul IV

### Intră, numărul 15788659/54377...

*Cei mai mulți dintre noi ne credem îndreptățiți să presupunem că toate datele și informațiile pe care statul le deține despre noi sunt protejate și că formularele pe care le completăm pentru Administrația Financiară sau pentru Biroul de Pensii rămân între noi și inspectorul nostru fiscal. Fișele cu starea sănătății noastre, am crezut întotdeauna, fiind atât de laborios puse pe hârtie de către medicul de familie, vor rămâne disponibile doar autorităților interesate și nu vor ajunge nicicum mai departe. Suntem încredințați că același lucru se va întâmpla și cu rapoartele păstrate de instituții precum Vamă și Accize. Evident, credem același lucru despre informațiile privindu-i pe copiii noștri, deținute de autoritățile educaționale locale, despre baza de date ADN sau de recunoașterea facială a poliției, Biroului de Informații privind Infractorii și multor alte arhive de date. Autoritatea pentru Șoferi și Autovehicule (DVLA) este în posesia unor cantități masive de informații despre noi și despre mașinile pe care le conducem, și ea publică analize nesfârșite și rapoarte savante privind obiceiurile noastre la volan. De fapt, majoritatea contactelor noastre cu statul sunt înregistrate și transcrise, informațiile putând fi folosite ulterior ca dovezi împotriva noastră.*

În fiecare zi din viață, intrăm în relație cu statul. Împrăștiem informații despre noi diferitelor agenții naționale. Fiecare vizită pe care o facem la medic este înregistrată în baza de date a Serviciului Național de Sănătate (NHS), în care evoluția sănătății noastre devine un grafic ce ne acoperă întreaga viață și este accesibil secretarului de stat și, de acolo,

oricui consideră acesta că trebuie să-i fie accesibil. Schimbările de domiciliu sunt înregistrate de către Administrația Financiară, DVLA și Departamentul Protecției Sociale, iar bunăstarea noastră este cunoscută de către bănci, companiile de scoring și agențiile de pensii. Baza de date națională computerizată a poliției și cea a Serviciului de Procuratură al Coroanei, dețin un raport complet, chiar dacă nu într-un totu corect, al istoriei noastre infracționale. Baza națională de date ADN are înregistrați în prezent două milioane de cetățeni britanici, iar numărul lor crește rapid. Telecom și companiile de telefonie mobilă dețin numeroase cunoștințe despre orice persoană adultă din Marea Britanie. De fiecare dată când utilizezi un telefon mobil, locația ta exactă este detectată, la fel ca și destinația apelului. Serviciile de utilitate publică au și ele cantități enorme de informații privind obiceiurile noastre cotidiene. Acum, când apa este contorizată în multe zone din Marea Britanie, companiile din domeniu îți pot spune chiar și dacă mergi regulat la toaletă în timpul vreunei emisiuni de televiziune populare.

Administrația Financiară încă se luptă cu dificultățile întocmirii unei baze de date imense, în care fiecare contribuabil din țară va fi înregistrat și confirmat de o altă sursă. Conform estimărilor curente, această bază de date va costa 30 de miliarde de lire sterline atunci când va fi completă, deși probleme de programare au tot pus piedici planului și, probabil, costul final va fi considerabil mai mare. Recenta fuziune dintre Administrația Financiară și Departamentul Vamă și Accize a creat potențial o unitate mult mai puternică de strângere a impozitelor, care va putea oferi o perspectivă cuprinzătoare asupra declarațiilor noastre de venit și să elimine anomaliile. Totuși, cum se întâmplă cu cele mai multe baze de date, eficiența sa va depinde de acuratețea datelor introduse și de abilitatea personalului de a o folosi. Chiar dacă informațiile sunt înregistrate detaliat, Administrația Financiară va fi mereu obligată să se bazeze pe formulare sau plicuri maro cu salarii și nu se poate aștepta ca toate impozitele declarate să fie precise. Ea nu doar strânge

taxe, ci îi forțează pe angajatori, în mod curent, să deducă rambursarea împrumuturilor studentești din salariile angajaților lor, obligând astfel întreprinderile să devină colectori atât de debite, cât și de impozite, în numele guvernului. Biroul de Pensii, care face și el parte acum din Administrația Financiară, are o bază de date specială, în care se regăsesc contribuțiile noastre la asigurările de stat, înregistrările locurilor de muncă și situația noastră financiară încă de la 16 ani. Cantitatea de informații oferite Administrației Financiare și înregistrate fără voia noastră poate fi confruntată și cu detaliile privind conturile noastre bancare și de economii și va fi pusă la dispoziția agențiilor de investigații precum Biroul pentru Combaterea Fraudelor Grave sau departamentul de colectare a taxelor al Administrației Financiare, aflat în Worthing. Desigur, aceste agenții nu se bazează numai pe datele aflate în acest mod, ci angajează și funcționari ale căror sarcini constau în investigarea contribuabililor și „pescuirea”, din istoria lor de salariați, a unor venituri frauduloase sau neconforme cu realitatea.

În 2004, Serviciul Național de Sănătate (NHS) a anunțat lansarea programului său de dezvoltare a unei baze de date computerizate. Contractele destinate acestui proiect, condus de departamentul IT al NHS, valorau inițial 6,2 miliarde de lire sterline. Cum era de așteptat, proiectul a depășit curând bugetul, costurile sale fiind estimate în 2005 la 31 de miliarde de lire. Acest program implică transferul unor ani întregi de fișe scrise de mână din înregistrările medicilor generaliști într-un computer național, aflat în Manchester. Transferul informațiilor va fi realizat cu precădere de experți IT externi. Conform declarațiilor lui John Hutton, ministrul Sănătății, guvernul oferea cetățenilor posibilitatea de a alege nivelul de securitate de care să se bucure dosarul lor. „Pacienții vor fi întrebați dacă doresc ca înregistrările lor medicale să fie incluse în baza de date sau dacă preferă ca aceste informații să fie scoase din sistem și protejate într-un «plic sigilat» electronic, care va restricționa accesul, exceptând cazurile de extremă urgență”. Ulterior, managementul acestui proiect a

modificat această garanție aparent liniștitoare, evidențiind faptul că pacienții care vor restricționa astfel accesul la propriile dosare își vor asuma riscul ca personalul clinic să mai și greșescă în situații de urgență. Împiedicarea accesului la înregistrări va fi sinonimă cu o cantitate mai mică de informații disponibile imediat despre probleme medicale cunoscute, inclusiv reacții alergice.

Baza de date a NHS va reprezenta una dintre cele mai complexe încercări de exploatare a datelor de până acum. Protecția sa este de importanță vitală pentru orice persoană din Marea Britanie care pune preț pe sfințenia vieții sale intime. Totuși, stă în puterea politicienilor și a funcționarilor publici să se asigure că nici măcar o informație medicală nu va ajunge pe mâini nepotrivite. Vor exista tot felul de legi, precum și amenințarea cu pedepse severe pentru hackerii care vor fi prinși înfruptându-se din aceste date. Guvernul a afirmat că această bază de date prezintă avantaje pentru noi toți, deoarece, grație ei, putem fi siguri că medicul care ne tratează are acces la cele mai recente și mai corecte informații ce ne privesc. Baza de date va fi mai protejată decât sistemul tradițional de hârtoage și ea nu va face parte din informațiile înregistrate pentru arhiva cărților de identitate. Oricum, profesioniștii din sfera sănătății au multe rezerve în privința acestui proiect. Înregistrările din domeniul sănătății publice ale britanicilor vor constitui o resursă neprețuită pentru industria asigurărilor sau pentru agențiile de menținere a liniștii publice. Industriile medicamentelor și asigurărilor sunt multinaționale și prospere, iar valoarea înregistrărilor medicale ale unei întregi națiuni li se va părea inestimabilă. „Dispozitivele de securitate” nu înseamnă mare lucru, fiindcă medicina de urgență poate deveni un proces haotic, ce solicită profesionalism clinic și tratament grabnic, așa că accesul rapid la înregistrări va fi prioritar. Probabil vor exista multe ocazii, în cadrul unei secții de urgență, în care securitatea bazei de date va coborî – și e de înțeles – pe lista priorităților. Vechiul sistem de informații scrise era mult prea greoi pentru ca persoane neautorizate să-l poată accesa facil, după bunul plac

și în profunzime. Nicio astfel de dificultate nu îi va stânjeni însă pe hackerii care vor să intre în baza de date a NHS. Va fi imposibil să protejezi datele în cazul unui accident ce ar aglomera o secție de urgență în care angajații împart un singur terminal de computer. Harold Cayton, de la Departamentul pentru Dezvoltarea Rapoartelor Medicale Naționale, a afirmat că împărtășirea informațiilor privind pacienții ar trebui să rămână o chestiune ce ține de relația medic-pacient. Departamentul se pregătește să publice o „Garanție a informațiilor medicale” (care, spune medicul meu, nu va valora nici cât hârtia pe care este tipărită!). Asociația Medicală Britanică (BMA) a solicitat guvernului asigurări și dispozitive de siguranță mai puternice. Unii medici generaliști și câteva cabinete medicale chiar au refuzat să-și predea înregistrările. Trebuie spus că pacienții nu au dreptul de a decide asupra datelor pe care doctorii le stochează, despre ei și că nu există niciun medic generalist sau vreun alt corp profesional care să fie în mod clar răspunzător de protejarea informațiilor strânse. Pare evident că multe dintre libertățile cetățenești vor fi puse în pericol.

Autoritatea pentru Șoferi și Autovehicule (DVLA) face parte din Departamentul Transportului. Autoritatea funcționează ca o bază de date computerizată încă din 1980, care ne emite permisele și ne procesează taxele rutiere. Ea reprezintă depozitarul înregistrărilor noastre auto și istoria mașinilor pe care le-am avut de-a lungul vremii. DVLA notează, de asemenea, adresele posesorilor tuturor autovehiculelor, polițele de asigurare, încălcările Codului Rutier și pedepsele primite pentru acestea, interdicțiile de a conduce, permisele provizorii și testele de conducere, precum și fișele de întreținere ale mașinilor noastre. Autoritatea caută mereu infracțiuni rutiere și condamnări, clasificate după sexul și vârsta celor ce le-au comis, precum și obligă la noi testări de după condamnări pentru conducere periculoasă sau sub influența alcoolului. Analizează statistici cu privire la recidive, pierderi de drepturi și supraviețuirea victimelor accidentelor. Examinează efectele pe care diverse medicamente și droguri le



au asupra șofatului și consiliază sistemul judecătoresc în privința verdictelor. Astfel, DVLA este implicată în administrația și legislația privindu-i pe toți șoferii din Marea Britanie. Arhiva sa este cuprinzătoare și este folosită constant de forțele polițienești din Marea Britanie și din străinătate.

Baza de date conține înregistrări ale mașinilor furate, informații ce sunt distribuite tuturor forțelor de poliție, prin sisteme de identificare a numerelor de înmatriculare. De asemenea, arhiva este în mod curent pusă la dispoziția companiilor de asigurări și a Sistemului de taxare antiambuteiaj din Londra. Software-ul pentru sistemul DVLA a fost instalat de către Capita, subcontractorul IT al guvernului, care a externalizat în India dezvoltarea de programe de arhivare, pentru a exploata forța de muncă ieftină din acest subcontinent asiatic. Organizațiile de apărare a libertăților cetățenești consideră că această mutare va face ca datele deținute de DVLA să devină disponibile în acest stat în curs de dezvoltare. Autoritatea are o experiență de decenii în prelucrarea datelor și pretinde că „securitatea informației este bine reglată”. Însă nu destul de bine. Au existat numeroase exemple de informații accesate ilegal prin computerul cu arhiva permiselor de conducere al DVLA și prin oficiul de verificări ale cazierului (CRB). Saul Dickinson, un apărător extremist al drepturilor animalelor, care a fost angajat al DVLA, a dat mai departe numele, adresele și numerele de înmatriculare ale personalului unei ferme de cobai din Staffordshire. Aceste informații au fost folosite într-o campanie de terorizare a familiilor care lucrau la fermă. Dickinson a fost condamnat la cinci ani de închisoare.

Lipsite de resurse, forțele polițienești din Marea Britanie primesc cu entuziasm revoluția tehnologică. Testările pentru arhiva ADN a poliției au fost privatizate și sunt luate mostre de la toate persoanele arestate sau implicate în orice fel în vreo infracțiune. În acest moment, există două milioane de indivizi incluși în această bază de date, iar numărul lor va crește rapid, ca urmare a modificărilor suferite de lege. Cei mai mulți din Arhivă nu vor fi niciodată condamnați pentru

vreo infracțiune, dar, după regulile curente, informațiile lor vor rămâne în baza de date cât vor trăi. Sunt luate mostre de salivă, fire de păr și fluide corporale, iar apoi comparate cu mostrele găsite la locul infracțiunii. Riscurile informațiilor ADN este că ele pot fi utilizate pentru a oferi date care n-au nicio legătură cu vreo infracțiune. De pildă, ele pot dezvălui amănunte ale unor relații de familie, inclusiv de paternitate, și predispoziții genetice pentru anumite boli, informații ce s-ar putea dovedi utile industriilor de medicamente și de asigurări. Genewatch, un grup de apărare a libertăților cetățenești îngrijorat de felul în care pot fi utilizate informațiile oferite de genomul uman, consideră că ar trebui să existe un corp public independent, transparent și responsabil, care să fie desemnat să ia decizii privind arhiva ADN. Mostrele ar trebui distruse după utilizare, spune Genewatch; trebuie interzise imediat cercetările genetice ce utilizează aceste date; în plus, eficiența acestei arhive în stoparea criminalității ar trebui analizată independent. Folosirea dovezilor ADN a dus deja la mari erori judiciare, în cazul unor femei acuzate că și-au vătămat propriii copii. Cercetările genetice au fost deja desecretizate. Un proiect numit Biobanca Marii Britanii intenționează să strângă și să analizeze datele genetice ale unui număr de 500.000 de voluntari cu vârsta de cel mult 30 de ani. Obiectivul este de a identifica acele gene asociate unor maladii – informații de mare interes, fără dubiu, pentru domeniul asigurărilor de viață.

Computerul Național al Poliției (PNC) reprezintă o bază de date ce acoperă întreg teritoriul țării și include condamnările pentru delikte „înregistrabile” – adică acelea pentru care vinovații pot fi trimiși la închisoare. Aceste înregistrări trebuie scoase din arhivă după zece ani sau după cinci ani, dacă persoana în cauză scapă pe cauțiune. De la trei condamnări în sus, înregistrarea rămâne în baza de date 20 de ani. Există, desigur, excepții, cum sunt persoane condamnate pentru infracțiuni de natură sexuală, acte violente, molestarea copiilor și persoanele fără discernământ care nu pot răspunde juridic pentru fapta lor. Arhiva PNC este disponibilă imediat

unui număr de aproape un sfert de milion de polițiști din Marea Britanie și este extinsă permanent. Un nou sistem de recunoaștere facială este evaluat în orașe din Yorkshire, Strathclyde, precum și de câteva forțe de poliție din regiunea Midlands. Recunoașterea facială a fost utilizată frecvent în alte părți, deocamdată fără succes. Ea presupune înregistrarea datelor biometrice faciale. Există 60 de părți ale feței identificabile separat, care formează împreună portretul unic al unui individ. Din nefericire, cam asta e tot. O fotografie pentru identificare a poliției, realizată și arhivată digital după o arestare, este clară, iar subiectul ei – imobil. Fața infractorului noaptea, în centrul plin de umbre al unui oraș, este cu totul altceva. În prezent, sistemul pare un experiment costisitor și eșuat. Totuși, multe milioane de lire sterline din bugetul autorităților locale de poliție au fost deja cheltuite și vor trebui justificate cumva. Tehnologia recunoașterii faciale nu a fost încă testată în tribunalele britanice, dar cum putem fi siguri că acest lucru nu se va întâmpla în viitorul apropiat, ducând la identificări greșite și erori judiciare?

În întreaga țară, poliția colaborează cu autoritățile educaționale locale pentru a pune capăt chiulurilor. Pentru prima oară în Marea Britanie, copiii-problemă au fost înregistrați pe computere, în multe zone ale țării. Când sunt prinși, chiulangiii „recidiviști” au mari șanse de a primi o „decizie de comportament antisocial”. În cazuri extreme, părinții lor pot fi – și unii chiar au fost – întemnițați. Stocarea datelor unor copii într-o arhivă națională reprezintă o problemă gravă. Organizațiile de apărare a libertăților cetățenești sunt îngrijorate că încă o barieră a fost dărâmată. Copiii sunt deja tratați ca infractori în Statele Unite, unde unei fetițe de cinci ani, care a avut un acces de furie în incinta școlii sale din Florida, i s-au pus cătușe și a fost luată din clasă de către ofițerii de poliție. Unii copii au mai fost închiși în Marea Britanie, dar includerea lor într-o bază de date a autorităților educaționale poate fi începutul unei periculoase spirale descendente. Deocamdată, nici chiar puștilor cu comportament deviant nu li se cere să poarte o carte de

identitate când vin – dacă vin – la școală.

Cărțile naționale de identitate sunt utilizate în toată lumea. Ele variază ca funcții și ca integritate a datelor, precum ajutoarele de sănătate sau asistența socială. Unele sunt obligatorii, altele nu. Unele utilizează numere pentru a identifica purtătorul, dar cele mai multe au încorporată o bandă electronică. Cardul de plastic a înlocuit „hârtiile” de identitate, fiindcă este mai greu de falsificat, iar producătorii de carduri știu să-și vândă marfa și pot cu ușurință să-și actualizeze în mod regulat sistemul, adăugând mai multe informații despre posesor și despre familia lui sau ei, pe măsură ce acestea devin disponibile. Aproximativ 100 de țări ale lumii au cărți de identitate obligatorii. Totuși, afirmația nu este valabilă pentru Statele Unite, Marea Britanie, Canada, Australia și Noua Zeelandă. În Australia și Noua Zeelandă, publicul a respins categoric, prin referendumuri, propunerea de introducere a unor cărți de identitate pe timp de pace. Canada a abandonat inițiativa unor cărți de identitate biometrice în 2004. Și, chiar și după atacul din 9/11, propunerile zgomotoase de introducere a unei cărți de identitate au fost respinse cu fermitate de Congresul Statelor Unite.

De obicei, cartea de identitate este introdusă într-o țară din rațiuni ce țin de rasă, politică, religie sau securitate. David Blunkett, fost ministru de Interne al Marii Britanii, a anunțat proiectul unei cărți de identitate „pentru drepturi” în octombrie 2001, imediat după tragedia de la turnurile gemene. Motivele sale erau de a înăspri măsurile antitero, îngreunându-le imigranților ilegali operațiunile din Marea Britanie, și de a contracara fraudarea ajutoarelor sociale. Cardul „pentru drepturi” urma să devină o carte de identitate obligatorie, chiar dacă nu era numit așa. Fiecare cetățean care îl solicita ar fi trebuit să plătească 75 de lire sterline și să ofere 50 de informații personale. Ideea a întâmpinat o opoziție imediată. Fostul secretar de Interne Mike O'Brian a spus: „Ministrii au admis deja că țelul nostru este de a căuta să apărăm libertatea și democrația. Fiecare împrejurare în

care suntem obligați să subminăm aceste valori va fi revendicată de teroriști ca o victorie”. S-a mai afirmat, pe bună dreptate, că existența cărților de identitate în Statele Unite nu ar fi putut împiedica atacul din 9/11.

Blunkett a bătut în retragere cu propunerea sa, însă a încercat introducerea cărții de identitate din nou în februarie 2002. După un baraj de critici venite din Camera Lorzilor, el a înlăturat formula ambiguă „pentru drepturi” și a descris cardul exact cum era gândit să fie – o carte de identitate. Mai mult, a admis că nu va fi obligatoriu să porți mereu acest card; totuși, el va fi cerut pentru a beneficia de ajutoarele de sănătate sau de asistența socială. Persoanele în căutarea unui serviciu vor trebui să prezinte cardul atunci când aplică pentru un loc de muncă sau alte „drepturi”. Inițial, Partidul Conservator a susținut introducerea cardului, apoi s-a răzgândit și s-a opus. Cei care s-au împotrivit proiectului au fost acuzați că sunt prea „moi” în fața amenințării teroriste – o greșeală politică fatală. Proiectul de lege a fost retras înainte de anunțarea alegerilor generale din 2005, deoarece nu mai era suficient timp pentru ca el să treacă prin Parlament.

Dacă acest card va fi sau nu impus vreodată în Marea Britanie, asta depinde, pe de-o parte, de cursul evenimentelor și, pe de altă parte, de introducerea unor schimbări ale altor documente de identitate, cum ar fi pașapoartele cu amprenta posesorului. Un alt factor este publicul: oare cetățenii vor înțelege în totalitate cu ce se vor confrunta dacă se decid să aplice pentru cartea de identitate? Cei mai mulți oameni cred că este o banală bucată de plastic, dar de fapt e vorba de un sistem vast, complicat și cu bătaie lungă, care implică un nivel de utilizare fără precedent a informațiilor personale.

Unii politicieni susțin hotărât ideea unei cărți de identitate naționale, însă avantajele lor de pe urma sistemului nu sunt nicidecum clare. Ce se va întâmpla cu adevărat când și dacă va fi introdus acesta? Este un proiect de lege cu țintă limpede. Mai întâi, va fi un Registru Național de Identificare, care îi impune ministrului de Interne obligația de a crea un Registru Central al Populației, conținând informațiile personale ale

tuturor cetățenilor britanici care au vârsta peste 16 ani. În al doilea rând, fiecărei persoane îi va fi alocat un număr unic, care va fi cunoscut ca Numărul Național de înregistrare a Identității (NIRN). Acest număr va reprezenta elementul-cheie care va permite agențiilor guvernamentale să acceseze și să împărtășească informații despre noi toți. Articolul 5 spune că trebuie să răspundem eventualelor cereri de a furniza date biometrice sau alte forme de identificare fizică, care pot fi o fotografie pentru recunoaștere facială sau imagini ale degetelor noastre arătătoare (utilizate în sistemul imigrării din SUA). Vom fi nevoiți să achiziționăm și să purtăm un card de plastic, care permite confruntarea directă cu informațiile din baza de date. Articolul 15 ne cere să prezentăm cardul ori de câte ori vrem să beneficiem de servicii publice. Iar articolul 6 afirmă că numărul „unic” și registrul vor fi utilizate de tot felul de agenții drept bază administrativă.

Va exista și o „componentă de confruntare” privind înregistrările de date, conform căreia toate agențiile guvernamentale au obligația de a se informa reciproc cu privire la modificările datelor noastre personale. Asta permite ca toate numerele noastre de înregistrare (precum cele de la serviciile naționale de asigurare sau de sănătate) să fie strânse laolaltă. De exemplu, dacă informăm Departamentul Protecției Sociale că ne-am schimbat domiciliul, acesta este obligat să anunțe Serviciul Național de Sănătate, poliția ș.a.m.d.

Articolul 19 al proiectului de lege permite divulgarea informațiilor din registru, fără a fi nevoie de consimțământul nostru, către – printre multe alte agenții – forțele polițienești, serviciile secrete, Administrația Financiară, Departamentul Vamă și Accize, Forțele de Muncă, Biroul de Pensii și Departamentul pentru Combaterea Crimei Organizate. Proiectul de lege va mai stabili o nouă gamă de infracțiuni. Și contravenții, creată pentru a se asigura că publicul îndeplinește cerințele cărții de identitate.

Dacă privim astfel lucrurile, vom realiza că nu vom avea doar un card simpatic de plastic, așa cum speram. Informațiile de care guvernul pretinde că are nevoie sunt detaliate și

reprezintă o intruziune în viața noastră. Aspectul poate cel mai alarmant al proiectului este faptul că nu conține nici o clauză conform căreia Parlamentul poate decide ce informații personale vor fi înregistrate în baza de date. Decizia este lăsată la latitudinea Ministerului de Interne, care va putea să suplimenteze numărul informațiilor solicitate după bunul său plac. Ministerul a declarat că va dori să știe despre fiecare unde am locuit în trecut (inclusiv adresele complete și codurile poștale) și că ne va solicita „informații despre împrejurările în care datele înregistrate (inclusiv fotografii, amprente, înregistrarea irisului, numărul de asigurare sau al pașaportului, carnetul de conducere și orice alt document oficial) au fost oferite altor persoane”.

Se produc, totuși, încălcări grave ale libertăților cetățenești, prin furt de identitate, în Marea Britanie și Statele Unite, cu toate că problema e mai puțin gravă în Europa. Germanii sunt încântați să poarte pretutindeni cărți de identitate și, la fel ca și toți membrii serviciilor armate din Marea Britanie, tolerează în general cerințele cardului, fiindcă s-au obișnuit deja cu ideea. Însă sistemul german reprezintă o intruziune mult mai mică în viața privată decât cel propus pentru Marea Britanie. Americanii sunt obligați să-și controleze viața și să-și conducă afacerile prin mijloace electronice. Lor li se cere mereu să dovedească faptul că sunt cine pretind că sunt. Practic, asta înseamnă că „elementele de date” personale sunt incluse în programele instalate pe mii de computere. Parolele, numerele de identificare fiscală, numele dinaintea căsătoriei, data nașterii, codurile poștale și alte informații individualizatoare sunt folosite pentru autentificare. Problema e că aceste detalii pot fi ușor accesibile hackerilor și, dată fiind răspândirea actuală a internetului wireless, dacă datele nu sunt criptate, ele pot fi accesate ușor de orice persoană din vecinătate care deține echipamentul potrivit și vrea să arunce un ochi în computerul tău. Fraudarea identității este marea problemă în Statele Unite. În 2002, FBI a arestat trei bărbați care furaseră 30.000 de rapoarte de scoring și le vindeau, pentru a fi folosite în diverse combinații de însușire abuzivă a

identității. Hackerii au mai izbutit să se infiltreze într-o companie care procesează tranzacții prin cartea de credit și au furat zece milioane de numere ale unor carduri Amex, Visa și Mastercard. Indiscutabil, vechile concepte confortabile de identitate privată nu se mai aplică în Statele Unite și Marea Britanie.

Astfel de infracțiuni sunt tot mai numeroase, deoarece prea multe informații personale ale noastre sunt disponibile pentru infractorii hotărâți. Așa cum am văzut până acum, zi de zi, ceas de ceas, agențiile de creditare, firmele de asigurări, băncile, supermarketurile și operatorii de carduri inteligente colectează informații despre noi. Iar apoi le vând. Cei care supraveghează și strâng date – în special companiile de evaluare a creditelor, precum Experian în Marea Britanie, sau neguțători de baze de date, precum Acxiom în Statele Unite – se opun reglementărilor guvernamentale și pretind că acestea ne-ar face viața mai scumpă și mai complicată. Creditele se obțin ușor. O companie americană numită Synovate, care urmărește solicitările de cărți de credit pe e-mail, afirmă că anul trecut au fost trimise în SUA înjur de cinci miliarde de oferte electronice.

În întreaga lume se află în circulație în prezent peste trei miliarde de carduri Visa și Mastercard, care generează profituri uriașe pentru companiile emitente. În mod corespunzător, hoții de informații au devenit din ce în ce mai pricepuți în evitarea măsurilor de protecție. În același timp, înregistrările agențiilor de scoring au fost viciate de erori, deoarece majoritatea informațiilor generate de operatorii de carduri au ca surse computere, nu oameni. Cele mai multe bănci de azi nu au casieri, manageri sau sucursale, iar datele sunt împrăștiate fără ca personalul specializat să le verifice mai întâi. Angajații costă bani, de care agențiile de scoring și companiile de creditare nu sunt dornice să se despartă. Unii oameni nu reușesc încă să înțeleagă de ce cartea de identitate a devenit o chestiune politică atât de sensibilă și atât de demonizată de apărătorii drepturilor cetățenești. Motivul este că lumea de azi e plină de informații personale, iar publicul



larg nu este dispus să semneze noi documente care ne leagă de mâini și de picioare, chiar mai mult decât suntem deja.

Introducerea cardului național de identitate a fost anunțată din nou într-un discurs al reginei din noiembrie 2004, iar propunerea a atras imediat critici. David Blunkett – a cărui relație amoroasă cu Kimberly Fortier, editoare a revistei *Spectator*, a suscitât interesul opiniei publice, atunci când informațiile despre, ea au apărut în presă – a declarat deja, într-o dezbatere a Camerei Comunelor din iulie 2002, că „este important să nu pretindem că o carte de identitate va deveni un factor cu rol hotărâtor în combaterea terorismului internațional. Eu nu am făcut afirmații privind contribuția lor substanțială în războiul antitero”. Totuși, în vara lui 2004, pe când discursul reginei nu era încă gata, tot el a declarat public că „un card de identitate ar avea o contribuție importantă la lupta împotriva terorismului”. Cum e posibil ca aceste afirmații contradictorii să fie făcute de un singur politician? Aproape că e un furt de identitate precum cele pe care cartea de identitate ar trebui să le combată. Desigur, era vorba de o declarație politică, emisă într-un context de isterie crescândă în privința posibilității unui atac terorist în Anglia.

Proiectul de lege a estimat că sistemul cărților de identitate va fi funcțional din 2008. Argumentele împotriva sistemului și a oricărui alt guvern care vrea să impună un card similar este că el schimbă irevocabil – și în rău – relația dintre individ și stat. Asta înseamnă că, efectiv, va trebui să cerem guvernului permisiunea să existăm. În cazul în care nu ne vom putea continua viața fără să folosim serviciile publice, fără să urmărim postul de televiziune BBC, fără să mergem la spital după un accident, fără să solicităm o pensie de stat. Formula sacră a legii și ordinii, „Inocenții nu au de ce să se teamă”, poate fi respinsă ușor, dacă ne amintim lecțiile pe care ni le-au oferit alte sisteme computerizate ale guvernului britanic, care s-au terminat dezastruos, cum sunt Agenția de Pașapoarte, Agenția pentru Ajutor în Creșterea Copilului, Biroul de Informații privind Infractorii – de fapt, mai toate inițiativele guvernamentale ce utilizau computerul.

Oriunde ar fi introdusă, cartea de identitate va crea instantaneu un nou strat de birocrație. Când îți duci copilul la școală pentru prima dată sau când îți vizitezi doctorul sau când devii membru al unui club de golf, cardul va trebui verificat de un portar, funcționar public, care va putea să-ți acceseze datele personale. Cartea de identitate îți va fi cerută cu ocazia unor „evenimente” majore din viața ta, cum sunt momentele când soliciți un permis de conducere, cont bancar sau pașaport; atunci, ochiul tău va fi scanat și comparat cu datele biometrice de pe card. Trăim într-o epocă în care deja suntem pe punctul de a ne îneca într-un ocean al legislației și al birocrației, iar cartea de identitate va crea noi valuri uriașe și costisitoare. Proiectul de lege include o clauză conform căreia poți primi o amendă deloc neglijabilă, de până la 1.000 de lire sterline, dacă omiți să declari la poliție că ți-ai schimbat domiciliul. Ce se întâmplă dacă pur și simplu uiți s-o faci? Proiectul de lege le cere prietenilor și vecinilor tăi să furnizeze informații despre tine.

Guvernul a justificat introducerea cărții de identitate, arătând că 35% din teroriști utilizează identități false. Asta înseamnă că 65% din ei n-o fac. Cum îi va opri cardul pe teroriștii islamici care vin la noi, așa, pentru a se odihni și relaxa? Cartea de identitate ar putea, într-adevăr, să reducă fraudele financiare, însă, în marea schemă a lucrurilor, asta reprezintă mult mai puțini bani decât sunt necesari pentru a finanța introducerea cardului, așa că nu se poate spune că-și va recupera cheltuielile. Guvernul estimează că instituirea sistemului va costa cel puțin două miliarde de lire sterline și probabil, în timp, costurile vor crește. Ministrul de Interne a afirmat în repetate rânduri că acest card va fi foarte important, punând accent pe siguranță, protecție, închiderea persoanelor periculoase la nevoie și menținerea lor sub control. Printre alte declarații, am fost asigurați și răsasigurați că sistemul va pune capăt turismului medical, cardul fiind utilizat pentru a se vedea cine este cu adevărat îndreptățit să fie tratat de Serviciul Național de Sănătate. Michael Wilkis, președinte al Comitetului de Etică din cadrul Asociației

Medicale Britanice (BMA), a răspuns acestei afirmații întrebând: „Ce proceduri vor trebui urmate în cazul unei urgențe, când pacientul nu are un card asupra sa? Ce implicații vor avea bolile infecțioase ale unor persoane care nu dețin o carte de identitate?”

E greu de înțeles de ce politicienii sunt atât de nerăbdători să impună publicului cărți de identitate, atâta timp cât în zilele noastre toți suntem înregistrați, cu cele mai mici detalii, în alte părți. Cunoașterea înseamnă putere, iar cardul este, evident, atractiv pentru un partid care crede în conceptul de „guvernare prin sprijin reciproc”. O bază de date unică, în care întreaga noastră istorie personală este accesibilă la o simplă „citire” a unui card poate părea o soluție ingenioasă și eficientă unui politician, dar și îngrozitor de intruzivă omului de pe stradă. Dar poate însăși denumirea „carte de identitate” ne deranjează atât de mult. Ce trebuie să faci pentru a-i dovedi că ești guvernului pe care l-ai ales? Adevărul este că, cel puțin în Marea Britanie, pașaportul britanic e pe punctul de a deveni într-un tot o carte de identitate, numai că nu se numește așa. Informațiile care pot fi accesate grație benzii electronice din noul document vor fi completate cu o amprentă. Pașaportul va costa 70 de lire sterline (în comparație cu 42 de lire, cât e acum), iar prețul i-ar putea crește până la 85 de lire dacă guvernul va fi obligat să includă planurile sale pentru cartea de identitate în sistemul pașapoartelor. Fotografia posesorului există deja. În 2006, cel puțin 600.000 de persoane, care solicitau pașaport, pentru prima dată au fost intervievate de Biroul Pașapoarte, iar numărul birourilor acestui departament a crescut de la șapte la 80. Personalul este acum de 500 de ori mai numeros. Foarte puțini știm exact ce date va conține banda electronică de pe pașaport. Conform Ministerului de Interne, mărirea numărului de informații incluse pe banda electronică este necesară pentru a combate fraudele din ce în ce mai sofisticate. Pe măsură ce amenințarea furturilor de identitate crește, țări din toată lumea înăspresc măsurile de securitate a pașapoartelor. Noua bază de date a pașapoartelor se va supune Legii

protecției datelor și, potrivit lui Simón Davies de la Privacy International, decizia finală privind informațiile incluse în pașaport depinde de soarta cărții de identitate.

Probabil cea mai importantă întrebare este dacă, în schimbul acestei puteri însemnate pe care le-o oferim, putem să avem încredere în cei pe care îi votăm că vor administra sistemul de identitate cu onestitate și eficiență. Pot ei garanta protecția datelor? Putem crede că ei ne vor spune adevărul în privința motivelor pentru care este necesar cardul? Vor înregistra oare în baza de date și informații despre noi asupra cărora nu vom fi înștiințați? Cum ne vom asigura că datele incorecte despre noi pot fi îndreptate?

Dacă ești cetățean britanic, se pare că numele tău va apărea în cel puțin 5 – 6 baze de date ale instituțiilor statului. Cu noile pașapoarte și eventualele cărți de identitate, lista lucrurilor pe care statul le știe despre noi se va mări considerabil. Baza de date ADN a poliției și cea imensă a Serviciului Național de Sănătate ne vor identifica după corpurile noastre sau după starea de sănătate. Cazierile noastre rămân unde au fost întotdeauna, numai că acum sunt disponibile la simpla atingere a unui buton. În ceea ce privește problema puștilor care trag chiulul de la școală și teama generalizată de molestare a copiilor, cât va mai dura până când fiecare copil din țară va trebui să poarte asupra sa un card și va fi înregistrat undeva într-un computer?

Eu cred că este doar o chestiune de timp.

<sup>1</sup> Criminal Records Bureau a fost înființat în 2002 în Marea Britanie pentru a verifica, înainte de angajare, cazierul potențialilor angajați, (n.red.)

## Capitolul V

### Distracții și jocuri de noroc

*Companiile de supraveghere își testează în mod curent produsele în cazinouri, deoarece trișorii sunt cei mai bine pregătiți adversari de pe piață. Există o unică metodă prin care se poate garanta câștigul într-un cazinou, iar acea metodă este trișatul. Nu poți învinge sorții niciodată. Chiar dacă mai pierd din când în când câte câte un milion de dolari în favoarea vreunui miliardar nesocotit aflat în trecere, cazinourile își recuperează pierderile pe termen lung, deoarece beneficiază de pe urma a ceea ce se cheamă „avantajul casei”: toate jocurile de noroc organizate de casă au de la bun început probabilitățile de partea acestora și împotriva jucătorului. Profitul mediu al unui cazinou se situează între 17 și 18%. Legea britanică a jocurilor de noroc este una foarte strictă. „Atențiile” nu sunt privite cu ochi buni. O masă gratuită din când în când, ori o mașină cu șofer, poate un pahar de șampanie – acestea sunt permise, însă prostituatele de lux, zborurile la clasa întâi și apartamentele la hoteluri de cinci stele sunt strict interzise în Marea Britanie. În alte țări, precum cele din Orientul îndepărtat și Africa, legislația este mai puțin severă. Unul dintre cele mai fascinante aspecte legate de industria cazinourilor este sortimentul bogat de trișori pe care i-a atras de-a lungul anilor. Câteva dintre cele mai strălucite minți din lume s-au dedicat încercărilor de a câștiga la cărți, la zaruri sau la ruletă, pentru că singurul mod de a câștiga pe termen lung este să încalci regulile. Aceasta este o înfruntare între cei care supraveghează și cei care schimbă puțin datele jocului.*

Cea mai concisă descriere a modului cum funcționează un cazinou este dată de Robert de Niro în filmul *Casino*, în care îl interpretează pe directorul unei luxoase săli de joc din Las Vegas. „Cum funcționează?”, este întrebat la începutul filmului. „În primul rând, îl ai pe crupier; apoi, e inspectorul care îl supraveghează pe crupier; după aia, pit boss-ul care îl urmărește pe inspector; managerul de etaj care îl urmărește pe pit boss. Eu stau sus și mă uit la managerul de etaj... în sfârșit, mai e și ochiul din plafon, care vede tot”.

Pe lângă probabilități, un cazinou se mai bucură de Alte două avantaje. În primul rând, dispune de banii necesari pentru a proteja „avantajul casei”, adică este capabil să achiziționeze orice sistem de supraveghere cunoscut omului și să angajeze cel mai competent personal de securitate. Apoi, dată fiind experiența unui secol de existență, toate trucurile din branșă sunt bine cunoscute. Cazinourile mari din Londra aduc experți care să-i învețe pe angajații responsabili cu securitatea cum ar putea fi duși de nas. Jucători străluciți de cărți, precum americanul Richard Marcus, unul dintre cei mai mari trișori din lume, care a străbătut lumea câștigând sume imense grație mâinilor lui de aur, oferă în mod regulat prezentări private în Londra. A studiat întreg arsenalul tehnic cu care s-a confruntat, a avut nervi de oțel și a înțeles psihologia personalului din camerele de supraveghere.

Nu poți păcăli camera de filmat. Este singurul lucru pe care te poți baza, fiindcă nu are inimă, nu are creier și, mai ales, nu joacă. În mod cert, nu te poți baza pe personal. Trebuie să accepți faptul că tot ce poate fi făcut pentru a învinge sistemul a fost făcut deja, cel puțin o dată, și va fi făcut din nou.

Coruperea crupierilor și a personalului de securitate s-a realizat cu succes de nenumărate ori, însă proprietarii de cazinouri învață din greșeli și implementează sisteme care să descurajeze tentativele de corupere a personalului; din acest motiv, toată lumea e supravegheată cu ochi de vultur. Multe cazinouri impun crupierilor să poarte șorturi – nu pentru a preveni murdărirea hainelor, ci pentru a face mai dificilă

strecurarea jetoanelor în buzunar. Uneori, personalul este percheziționat la sfârșitul turei, iar în unele state din SUA, jetoanele conțin dispozitive de urmărire, astfel încât șeful să știe unde îi ajung banii.

Sistemele neurale pentru depistarea și evidențierea anomaliilor din tiparele de comportament au fost utilizate pentru prima oară în Marea Britanie de Ladbrokes. Mișcările din cadrul unui joc de noroc sunt previzibile prin aceea că respectă un set de reguli. De pildă, odată încheiat procesul de pariere, nimeni nu mai poate atinge jetoanele de la masa de joc. Același lucru se aplică tuturor jocurilor, inclusiv celor de blackjack (21) sau zaruri. Un sistem neural orientat către pânza mesei de joc poate surprinde și scoate în evidență un pariu întârziat ori îndepărtarea unei sume pariate înainte ca rezultatul să fie anunțat de către crupier. De îndată ce aceasta se întâmplă, personalul de pază se prezintă la fața locului, iar jucătorul în culpă este oprit. Richard Marcus și-a luat sistemul drept aliat atunci când a descoperit că anumite combinații de culori ale jetoanelor anihilează sistemul neural într-o lumină artificială. Această descoperire i-a adus frumoase sume de bani. În cazinourile dotate cu supraveghere contra măsuirii mizelor, Marcus pune a miză și o muta doar atunci când nu câștiga. Echipa sa era formată din trei membri, cu ajutorul cărora afla instantaneu numărul câștigător la ruletă și, în cazul unui eșec, își recupera jetoanele, în mijlocul haosului creat de solicitarea de plată a câștigurilor de către ceilalți participanți la joc.

Fabricanții de echipamente au fost, de-a lungul timpului, mituiți pentru a modifica modul de funcționare al ruletei sau al zarurilor. Cărțile se pot marca, se pot monta computere și camere de filmare pe podea pentru a stabili avantajul casei, se pot fixa magneti pe masa de ruletă. Dorința disperată de a învinge, măcar o dată, cazinoul și de a câștiga ceva în schimbul a nimic pare să-i obsedeze pe mulți din cei care au drept pasiune jocurile de noroc și să planeze mereu ca o amenințare asupra industriei. Toate cazinourile mari au luat măsuri de protecție. Podeaua este filmată și supravegheată 24

de ore din 24, mesele sunt testate cu cele mai performante cumpene, roțile ruletelor sunt echilibrate și controlate periodic, pachetele de cărți sunt livrate cu ajutorul furgonetelor securizate și puse spre păstrare în seifuri.

Jocurile de noroc sunt un viciu. Când merge din ce în ce mai rău și parcă ești posedat, nu mai e vorba doar de dorința de a câștiga, de a deveni miliardar cu iahturi, avioane private și femei frumoase. O miză devine ca un drog. Pentru mulți, reprezintă o senzație apropiată de cea pe care o ai în timpul sexului. Un debușeu scurt după o perioadă tensionată, care parcă nu se mai termină. Pentru unii, atracția o reprezintă ucigătoarea așteptare de după încheierea pariurilor, când inima îți stă în loc – trei minute de groază, în care nici nu mai respiri, așteptând ca bila albă să se oprească din goană în dreptul unui număr anume. Sau întoarcerea ultimei cărți, când inima îți bate să-ți sară din piept și mâinile nu se mai opresc din transpirat. Pentru alții, rezultatul nici nu contează prea mult. Importante sunt emoțiile care însoțesc scurgerea printre degete a ultimelor rămășițe ale averii moștenite. Euforia jocului, a câștigului și a eșecului, vine după ani și ani de pariat la întâmplare, de extaz și de agonie. De asemenea, se prea poate ca țelul să fie câștigul. Câștigul cu orice preț. Tocmai împotriva acestei dorințe se înverșunează, cu toate resursele de care dispun, supraveghetorii. Personalul cazinourilor nu este angajat niciodată fără ca dosarele să fie analizate în prealabil cu cea mai mare atenție, și cele mai multe săli de joc recurg la companii precum Lexisnexis pentru a obține aceste informații pentru toți angajații.

Alții știu că există metode de a învinge casa. Sunt școli în America în care absolvenții de facultăți cu profil real sunt antrenați în arta de a număra cărțile la blackjack. Ai nevoie doar de multă inteligență, de o memorie redutabilă, de răbdare și de puterea de întoarce avantajul împotriva casei, prin cunoașterea întocmai a poziției fiecărei cărți din teancul crupierului. Problema derivă din aceea că există șase pachete de cărți în teanc. Pe de altă parte, „numărătorii” nu s-au născut de ieri, de azi. Aceștia joacă 21 cu o frecvență care



depășește puterea de imaginație a celor mai mulți dintre noi, așa că sunt prinși și devin *persona non grata* atunci când se lăcomesc sau când pit boss-ul și supraveghetorii din camerele de deasupra îi recunosc după tiparele lor de joc. Câteodată, identificarea se realizează cu ajutorul programului de recunoaștere facială, instalat pe sistemul de supraveghere cu circuit închis. Ocazional, se poate afla dacă cineva care câștigă suspect de mult a fost vreodată evacuat din alte săli de joc.

Software-ul biometric de recunoaștere facială este utilizat în mod regulat de sălile de joc americane. Caesar's Palace din Las Vegas nu doar îl folosește, ci îi și face reclamă, iar multe cazinouri britanice l-au testat. Sistemul este foarte popular în Statele Unite, dată fiind decizia guvernului de a-l utiliza ca măsură aniteroristă, ceea ce a crescut în același timp investițiile în tehnologie. Capul securității dintr-un cazinou londonez din Curzon Street mi-a mărturisit că, în opinia sa, recunoașterea facială se realizează cu mai mult succes de către personalul angajat. „Recepționiștii noștri au o memorie redutabilă și s-a dovedit că deciziile lor de a permite sau nu accesul unui jucător în cazinou sunt mult mai de încredere decât orice nouă tehnologie. Pariorii dați afară se vor întoarce, mai devreme sau mai târziu, deghizați și cu identități false. Niciun sistem de supraveghere nu va sesiza așa ceva. Noi ne bazăm pe instinctul angajatului.

Știu din surse de încredere că sistemul de recunoaștere facială de la Caesar's Palace funcționează anapoda. Sunt mii de jucători, și; chiar atunci când monitoarele indică ceva, tot trebuie să trimiți oameni să rezolve situația. Nu e întotdeauna simplu și, în opinia mea, nu e o tehnologie în care să te poți încrede”.

Primul lucru de care îți dai seama când intri într-un cazinou este că ești supravegheat, și ești lăsat intenționat să îți dai seama de asta. Camerele sunt pretutindeni și fiecare mișcare îți este înregistrată cu imagini de cea mai înaltă calitate. Peste tot e câte un pit boss sau manager de etaj – bărbați cu privirea rece, îmbrăcați la patru ace, care supraveghează jocurile și jucătorii. Crupierii își fac treaba cum

pot mai bine, încercând în același timp să prevină măsluirea mizelor, retragerile jetoanelor ori schimbarea poziției acestora. Orice joc de noroc necesită utilizarea unei anumite tehnologii de bază. De pildă, roata ruletei este verificată și echilibrată regulat, astfel încât, atunci când se învâрте, să nu existe posibilitatea de influențare a probabilităților. Pachetele de cărți îndeplinesc un standard întotdeauna același, iar jetoanele sunt imposibil de reprodus. Mișcările suspecte sunt sesizate imediat, dacă se utilizează tehnologia neurală ori dacă pit boss-ul observă ce se întâmplă. „Dar oricât de performantă ar fi tehnologia utilizată, tot ai nevoie de oameni la fața locului”, susține sursa mea de pe Curzon Street. „Sistemul neural este impresionant și te anunță instantaneu, dar tot e nevoie să ajungi la sursa problemei în timp util. Oricât de eficient ar fi modul de comunicare, aceasta se poate dovedi foarte dificilă într-un cazinou aglomerat”.

Desigur, industria, nu e ferită de anomalii. De pildă, în Marea Britanie, echipamentul folosit de cazinourile din provincie este adesea inferior celui de ultimă oră din Crockfords sau Les Ambassadeurs. Cazinourile cu ștaif din Londra utilizează cel mai bun echipament de pe piață, solid și rezistent la uzură, cu părțile din lemn măiestrit lucrate și încrustate, cu axul și rulmenții gândite și puse în practică de meșteșugari adevărați. De cealaltă parte a balanței, în orașele de provincie, cu cote inferioare, în care jucătorii nu se așteaptă să găsească luxul cazinourilor din alte locuri, standardele dotărilor din sălile de joc lasă adesea de dorit. În 2004, patru oameni au devenit indezirabili în cazinourile din Midlands, după ce au pus cu succes în practică „schema grăsanului”. Deși camerele de supraveghere au înregistrat după un timp incidentul, detectarea acestuia a durat ceva. Schema necesită trei jucători. Un bărbat solid apare, cu un număr mare de jetoane de valoare mică, și se așază la capătul mesei, cât mai departe de ruletă posibil. Cei doi complici, a căror prezență bărbatul o ignoră, încep să joace, observând cu atenție tiparul numerelor, în timp ce ruleta este în mișcare, în prealabil, cei trei au putut observa că suprafața pe care ruleta

se află și ruleta însăși sunt atașate unei plăci lemnoase nu foarte stabile, a cărei suprafață poate fi modificată de o persoană având o greutate considerabilă, formând astfel un unghi menit să influențeze ruleta.

De-a lungul câtorva ore în care grăsanul și-a odihnit burdihanul la capătul mesei, cei trei au putut stabili un tipar de modificare a unghiului favorabil lor. Odată stabilită tehnica eficientă, este vital ca trișorii să nu devină prea lacomi. Tiparele de pariere, câștigurile și pierderile sunt permanent înregistrate și transformate în grafice în cazinouri, oricât de mici ar fi aceste cazinouri. Dacă modul de joc sfidează în mod suspect avantajul casei, atunci ceva e în neregulă și supraveghetorii intră în alertă. Cei trei nu au stat locului, căutând permanent alte cazinouri cu dotări vulnerabile în fața unui supraponderal. Pe măsură ce și-au perfecționat tehnica, au început să câștige tot mai mult. Au fost prinși în Leeds de un supraveghetor vigilant, care, când și-a dat seama din înregistrările camerelor cu cine are de-a face, a instalat o cameră cu lentile din fibră optică pe un pilon din apropierea mesei. Desigur, nu a obținut cine știe ce dovadă (rareori se găsesc astfel de dovezi), însă industria răspunde întotdeauna la fel atunci când are certitudinea că unii din clienții lor umblă cu ocaua mică. Îi filmează, îi dau afară și le interzic să revină, scriu o descriere a escrocheriei și o răspândesc în întreaga branșă, dimpreună cu fotografiile celor implicați.

Arhivele celor mai multe companii de jocuri de noroc sunt meticulos organizate. Așa și trebuie, pentru că, prin forța lucrurilor, la mijloc sunt banii acționarilor, deci o chestiune sensibilă pentru ei. Crockfords, de pildă, ține înregistrări privind orice jucător suspect, devenit persona *non grata* oriunde în lume.

Personalul de securitate angajat în branșă este intransigent și calificat corespunzător. Șeful securității de la Crockfords s-a alăturat companiei după ce a ieșit la pensie din cadrul poliției metropolitane ca superintendent-șef, al doilea grad ca importanță în cadrul poliției britanice, unde era șeful Diviziei

Cluburi și Vicii la secția din Charing Cross. Ajutorul său este fostul său subaltern, un inspector-șef care derula operațiuni împotriva cluburilor din West End. Aceleași standarde nu sunt, însă, valabile pentru toată industria. Unii angajați au mai multă experiență decât alții. Supraveghetorii au experiență în legile care guvernează jocul în sine. Le-au văzut pe toate, din acest motiv au fost angajați. De-a lungul carierei lor de oameni ai legii, ei îi vor fi băgat la răcoare pe unii dintre cei mai abili escroci.

Jocurile de noroc sunt o afacere globalizată. Cei împătimiți călătoresc în lumea întreagă doar pentru a juca. Duc o viață de huzur și caută acele jocuri unde îi găsesc pe alții asemenea lor. Sunt jucători de cărți, cel mai adesea de pocher sau de blackjack, și preferă locurile unde poturile sunt nelimitate, iar directorii – persoane discrete. Modurile de a trișa sunt la rândul lor internaționale, deoarece escrocii trebuie să găsească permanent țări unde încă nu sunt cunoscuți și pot să o ia de la zero. Industria cazinourilor se află în plină creștere, săli imense deschizându-se în Australia, Africa de Sud și Orientul îndepărtat. Introducerea unei noi tehnologii înseamnă noi dificultăți pentru industrie. Cazinourile britanice și americane, deși au considerat identificarea prin frecvențe radio (RFID) ca pe un nou mod de a supraveghea traseul jetoanelor și de a preveni utilizarea improprie a bunurilor proprii ori spălarea de bani, nu s-au grăbit să investească în coduri de bare radio, din cauza costului ridicat al acestei tehnologii. Pe de altă parte, americanii și-au instalat în cazinouri toate sistemele tehnologice cunoscute omului, inclusiv pe cele de urmărire. Trișorii nu se sfiesc să utilizeze potențialul oferit de mijloacele electronice pentru a transmite, în mod discret, informații pe distanțe scurte. La începutul lui 2005, opt infractori thailandezi au fost arestați în Popiet, un sat de vacanță din Cambodgia, apropiat de granița cu Thailanda și de orașul Chiang Mai. Ei fuseseră prinși după ce au câștigat, cu sprijinul unui dispozitiv electronic, 90 de milioane de bath (peste 1, 2 milioane de lire sterline) la blackjack, în cazinoul Star Vegas. Personalul de securitate a declarat că aceștia montaseră

microcipuri în jetoanele de joc, ceea ce le-a permis să scaneze cărțile și să transmită mai departe datele către un laptop dintr-o cameră de hotel. Complicii aflați acolo îi contactau apoi pe telefonul mobil, oferindu-le, prin mesaje codate, informații despre cărțile de joc.

Importanța ochiului electronic este greu de estimat, deoarece el are preponderent un rol preventiv. Americanul Richard Marcus a trăit ani buni de pe urma escrocheriei sale la ruletă, pariarea pe coloana cunoscută drept „19-le prin 36”. Aceasta nu era niciodată sesizată de camere, deoarece pariarea se făcea cât mai departe posibil de crupier și, de îndată ce bila albă se oprea în dreptul unui număr, Marcus urma să ascundă miza, în cazul în care aceasta includea, printre celelalte jetoane, unul cu valoare mare, sau să o păstreze, dacă suma pariată nu era una semnificativă. El și-a botezat schema „Savannah” și plănuia să joace o „Super Savannah” la cazinoul Horseshoe din Las Vegas, către sfârșitul carierei sale. Dacă aceasta s-ar fi dovedit de succes, i-ar fi adus 1.050.000 de dolari. Marcus a renunțat, însă, dat fiind că șansele la ruletă de a ghici numărul câștigător sunt de 37 la 1 și ar fi trebuit să parieze 30.000 de dolari pentru a câștiga. Ar fi trebuit și să recurgă la măsluirea mizei, dar poate ar fi fost nevoit să o facă de mai multe ori. Știa că, dacă i-ar fi mers, cei de la supraveghere ar fi început să se uite cu atenție pe casele cu înregistrări și că astfel ar fi fost prins. Așa că a ieșit la pensie, deși nu poți să nu te întrebi: „S-a retras cu adevărat?” sau „E într-adevăr atât de priceput pe cât susține că este?”

Utilizarea RFED, deși a dat amploare încercărilor de identificare a trișorilor din industria jocurilor de noroc, este implementată cu mari dificultăți în Marea Britanie, din cauza costurilor pe care le presupune. Un grup de patru albanezi a fost arestat la Ritz Casino din Londra în 2004, după o plângere a personalului de supraveghere. Câștigaseră între 2 și 3 milioane de lire sterline, folosindu-se de un celular modificat și de tehnologia laser pentru a influența modul de funcționare al ruletei. Poliția nu a putut dovedi nici ce s-a întâmplat, nici

că s-a întâmplat ceva. Telefonul mobil a fost demontat și examinat de specialiștii de la Nokia. Arestarea a fost în principal rezultatul schimbului de informații cu cazinouri din Franța și Italia, de unde est-europenii plecaseră, de asemenea, cu buzunarele burdușite. Convinși de faptul că fuseseră trași pe sfoară, cei de la Ritz au refuzat să plătească sumele câștigate, însă investigația oficială s-a stins de la sine, când anchetatorii nu au reușit să prezinte nici măcar o probă fizică a producerii infracțiunii. Suspiciunile nu cântăresc prea mult într-un tribunal, așa că, după șase luni de inactivitate și frustrări, jucătorii și-au primit banii. Au părăsit țara și, fără doar și poate, acum golesc seifurile cazinourilor undeva prin Orientul îndepărtat.

Jocurile de noroc atrag personalități puternice. Pentru a fi bun, trebuie să ai nervi de oțel, să-ți meargă mintea, să știi care-ți sunt șansele și să ții pasul cu noile tehnologii, mai ales acum, în epoca microcipurilor și a sistemelor sofisticate de supraveghere. Pentru a fi un jucător excelent, trebuie să fii 100% hotărât să câștigi și să ai un orgoliu ieșit din tipare. Donald Trump, proprietarul Turnurilor Trump din Atlantic City, vrând să dețină cazinoul aflat la cea mai mare înălțime din America, s-a confruntat cu următoarea piedică: hotelul său avea doar 48 de etaje, un număr insuficient pentru ambițiile sale. Astfel încât a modificat modul de funcționare al liftului, iar acum etajele de la 2 la 9 lipsesc, pentru ca el să se poată lăuda cu un cazinou la etajul 54. Asta înseamnă enorm pentru el.

Detectarea utilizării „numărării” la blackjack se face prin verificarea computerizată a tiparelor de joc. Școlile unde se predă „numărarea” la blackjack se mută din hotel în hotel, deghizate în cursuri de contabilitate. Tarifele pot ajunge la 15.000 de lire sterline pentru un curs de două săptămâni, și cursanții fac grosul muncii, de-a lungul a zece zile de dificil calcul matematic și de practică. O școală cu renume în zona Las Vegas predă de asemenea măslirea mizei și cursuri de „mână ușoară”. Un „numărător”, odată ce și-a dat seama unde se află cărțile mai mari, pune o unică miză cu valoare mare

înainte de a se retrage. Potrivit unui responsabil cu securitatea, detectarea se poate realiza numai prin intermediul personalului, care l-ar putea recunoaște pe „numărător” și prin stilul său de joc. Unele metode nu pot fi surprinse de camerele de supraveghere, ci numai de sistemele de calcul matematic al tiparului de joc.

În ceea ce privește mijloacele de supraveghere ale cazinourilor, frapază faptul că, în lipsa unui sistem neural, deoarece numărul de camere care înregistrează toată activitatea din sală este prea mare, nu toate pot fi privite. Arhivele televiziunii cu circuit închis sunt examinate, de regulă, numai atunci când se înregistrează probleme, iar crupierul crede că are de-a face cu o escrocherie. Măsluirea mizei la blackjack este probabil cea mai iscusită metodă, se cere a fi executată rapid, dar va fi pusă în aplicare la neșfârșit, atâta timp cât jocul are loc în cazinouri. Odată depistată de crupier, va fi confirmată de înregistrări, așa că toate eforturile trebuie concentrate în direcția adormirii vigilenței personalului. Sunt șapte secțiuni de joc la masa semicirculară de blackjack. Crupierul stă cu fața la jucători, în centru, în spatele semicercului. Măsluirea mizei necesită o mișcare ritmică simplă. Jucătorul se așază la masă în timp ce crupierul strânge cărțile, după plata pariurilor câștigătoare. Mai întâi, el plasează trei jetoane roșii de cinci lire în poziția din extrema dreaptă a crupierului. Asta presupune ca, după jucarea mâinii, jucătorul să fi fost ultimul care a pariat și să fie primul plătit în caz de câștig. Sau primul căruia i se iau jetoanele în cazul în care pierde, în timp ce se așază, pune cinci jetoane negre de 50 de lire sterline pe pânza verde, în dreptul său, și le acoperă cu mâna dreaptă, astfel încât nimeni altcineva din cazinou să nu le vadă. Între degetul mare și cel arătător ale aceleiași mâini, el ține două jetoane „de mișcare”. În buzunarul din stânga are alte două duzini de jetoane roșii. Cărțile le joacă cu mâna stângă, lipite de stofa mesei, iar atunci când se ridică, strecoară cărțile sub jetoanele roșii. Dat fiind că joacă în extrema dreapta a crupierului, la sfârșitul mâinii el nu va putea fi văzut de restul celor de la masă. Poziția din dreapta

permite formarea unui unghi mai larg între mâna crupierului și cercul de jucători.

Jucătorul care recurge la o astfel de escrocherie evită cu orice preț opțiunea de a-și dubla miza, deoarece nu dorește să se afle într-o situație de verificare a mizei inițiale, când crupierul îi poate număra din nou jetoanele. Cărțile au fost strecurate sub cele trei jetoane, jocul își urmează cursul corect, iar trișorul pierde. Folosindu-și doar mâna stângă, el mai ia trei jetoane din buzunar și le plasează în extrema stângă a cercului de pariuri, din nou lângă mâna dreaptă a crupierului. Își păstrează mâna dreaptă pe masă. Câștigă următoarea mână cu o pereche de regi, în timp ce crupierul și unul sau doi dintre jucători depășesc pragul de 21. Crupierul întoarce cărțile și plătește imediat suma corespunzătoare celor trei jetoane roșii. În timp ce el se întoarce către ceilalți jucători, trișorul retrace cele trei jetoane inițiale pe care pariase, în timp ce, cu mâna dreaptă, strecoară două jetoane negre de 50 de lire sterline sub cel roșu de deasupra, plasându-le exact acolo unde fuseseră jetoanele lui inițiale. Cu aceeași mișcare, scapă cele trei jetoane roșii în buzunarul din stânga al sacoului, atenționându-l cu mâna dreaptă pe crupier: „Nu te supăra, cred că nu mi-ai dat cât trebuie”, răsturnând pe masă turnulețul cu două jetoane negre și unul roșu.

Când managerul de etaj se prezintă la fața locului, are în față miza de 205 lire sterline, cu jetoanele negre de pe masă. Am văzut cu ochii mei cum se execută această manevră pe televiziunea cu circuit închis și nu am putut-o depista, date fiind relaxarea și viteza cu care a fost făcută. Este o îmbinare de dexteritate și de cunoaștere a psihologiei. Nici supraveghetorii nu au depistat-o decât la câteva săptămâni după ce a avut loc. Jucătorul a avut ghinion și a fost pus pe lista neagră. Când va mai dori să joace, va trebui să se întoarcă în Statele Unite, adică acolo de unde a venit.

Cum jocul de zaruri utilizează serviciile a doi angajați, el necesită colaborarea a trei trișori. Masa este mai mică, iar crupierii – mai aproape de jucători și mai vigilenți. Dacă cel care aruncă zarurile nimerește un 7 sau un 11, a câștigat. Un



2, un 3 sau un 12 înseamnă înfrângere. În orice altă situație, corespunzătoare unor „puncte”, zarurile trebuie aruncate din nou, până la un 7 câștigător. Dacă 7-le iese primul, jucătorul pierde, iar crupierul se alege cu jetoanele. Cele mai multe mese de zaruri sunt atent supravegheate, dat fiind caracterul haotic al acțiunilor care însoțesc jocul.

Cei trei trișori de la un joc de zaruri sunt Pariorul, Revendicatorul și Detectivul. Pariorul pune la bătaie trei jetoane roșii.

În cazul în care câștigă, el schimbă cele trei jetoane cu altele „de mișcare” – două vișinii și unul roșu deasupra. Se folosește de ambele mâini, ridicând miza inițială cu stânga și înlocuind-o, instantaneu și exact în același loc, cu dreapta. Mișcarea se cere a fi continuă și rapidă. Odată efectuată substituirea, intră în joc Revendicatorul, care așază un turnuleț „de rezervă” cu jetoane vișinii la marginea mesei, în sectorul destinat mizelor. Crupierul, care anunță rezultatul aruncării, și supraveghetorul așezat între jucători, al cărui rol este acela de a observa cu atenție desfășurarea jocului și împărțirea câștigurilor, nu îl vor fi observat pe Revendicator până când acesta nu începe să protesteze că nu a fost plătit îndeajuns. Motivul acestei mișcări este că Pariorul a tot mizat constant, până la acest joc, câte 15 lire sterline. Dacă el ar anunța deodată un pariu câștigător de 2005 lire sterline, ar suscita suspiciunea angajaților cazinoului. Un jucător nou care ar face asta ar fi mai ușor de acceptat.

Angajații cazinoului londonez cu care am discutat au căzut de acord asupra faptului că sistemele neurale oferă unica soluție viabilă la măslirea mizelor, deoarece atrag instantaneu atenția asupra incidentului. Pentru sistem, mișcările din jurul unei mese de joc nu au nicio valoare, cu excepția situației în care toate camerele care înregistrează jocul sunt acoperite cumva, ceea ce este foarte greu de realizat. Masa de zaruri este, la fel ca și cea de ruletă, una cu foarte multă mișcare, și, chiar cu doi angajați la masă, o substituție se poate realiza fără să bage cineva de seamă. Prin natura sa, jocul este unul rapid, cu un ritm al său. Orice

decizie a unui responsabil cu securitatea de a nu accepta un pariu este dificil de luat. Mai greu cântăresc motivele pentru care cazinoul mai degrabă ar plăti și jocul ar continua, însă cea mai mare greșeală a trișorilor ar fi să se lăcomească și să încerce din nou.

Cel de-al treilea membru al echipei este Detectivul, care trebuie să se asigure că în zonă nu se mai află și alți angajați însărcinați cu securitatea ai cazinoului și că pit boss-ul nu urmărește jocul. Echipele de profesioniști au un limbaj prin semne propriu, iar cei doi jucători care au făcut schimbarea stau tot timpul cu ochii pe Detectiv. Acesta poate utiliza coduri precum un strănut sau un semn cu ochiul pentru a amâna manevra. În caz de nevoie, îi poate ajuta pe Parior și pe Revendicator să părăsească în grabă cazinoul. Detectivul nu trebuie să scape din ochi atitudinea personalului și să apreciez vizual întreaga atmosferă din sală.

Aici sistemul de televiziune cu circuit închis devine neputincios. Pe bună dreptate, cazinourile acordă o importanță aparte căilor de ieșire din clădire, deoarece pe acolo nu numai jucătorii, ci și banii părăsesc sala. Nu doar asociații, ci și clienții preferă să știe că este imposibil ca o șleahță de haidamaci să blocheze, ușa și să înceapă să îi scuture de bani. Problema sistemelor de supraveghere este că ele nu pot prezice ceea ce urmează să se întâmple: ele înregistrează, nu fac previziuni. Sistemele neurale de ultimă oră pot ajuta privitorul să ia o decizie în legătură cu o situație complicată, însă întâmplările se succed al naibii de repede în sala de joc, mai ales dacă trișorii au și o strategie de ieșire. De obicei, există o singură cale de acces în clădire. Dacă situația devine critică, echipa va face tot posibilul să ajungă la recepție și de acolo să iasă în stradă, unde cei trei se pot despărți și pot fi în siguranță. Dacă este prins și își știe meseria, un jucător profesionist nu va ciripi nimic până când nu este eliberat sau își poate suna avocatul. Dar dacă scapă și îl țin nervii, trișorul mai poate sta pentru un ultim joc, punând ca miză un jeton roșu și două violet și plecând apoi, fără a mai aștepta deznodământul. Aceasta l-ar face pe supraveghetor,

care poate și-a dat seama că a fost fraierit, să se simtă mai bine și să uite ceea ce tocmai s-a petrecut.

Pe de altă parte, se prea poate să nu o facă.

## Capitolul VI

### Aude-tot, vede-tot

*Pentru oameni ca noi, spionii sunt niște creaturi fascinante. Îi asociem cu un stil de viață exotic și îi invidiem pentru abnegația cu care, calm și discret, își văd de treaba lor, apărând interesele naționale. Însă comunitatea agenților secreți este un mecanism uriaș și greu de manevrat, care se infiltrează în toate colțurile lumii noastre. MI5, oficial cunoscut pur și simplu ca „serviciul de securitate”, se află în linia întâi a luptei împotriva terorismului din Marea Britanie și este în plin proces de dezvoltare a unei rețele de birouri regionale și de recrutare a o mie de ofițeri noi. MI5 este puternic, dar nu este corect să ne referim la el ca la o organizație de poliție secretă, deoarece nu are puterea de a aresta. Pentru asta se bazează pe poliție și departamente precum Vamă și Accize. Cu toate acestea, MI5 exercită o putere imensă, putând pătrunde peste tot și instala microfoane după bunul plac. Niciodată până acum serviciile secrete nu au dispus de o asemenea putere. Și, desigur, „umbrele” autohtone nu sunt singurii agenți de informații care operează în țară – mai avem și spioni străini. Americanii adună informații despre telecomunicații, iar francezii nu îi scapă din ochi pe teroriștii „locali” – atât ai noștri, cât și ai lor. Spionajul n-a fost niciodată atât de multinațional și atât de sofisticat tehnologic ca acum. Spionii sunt plasați în vârful ascuțit al aparatului de stat camuflat și au acces la toate secretele noastre.*

Oricine se afla în America în jurul datei de 11 septembrie 2001 își amintește cu siguranță schimbarea vădită care a cuprins țara – un amestec de șoc și teamă. Lucram pe atunci la

Universitatea din Pittsburgh. Părea că, din senin, străzile s-au golit, iar aerul curat fusese absorbit din însoritele după-amiezi de vară târzie. Ca englez, nu mă simțeam în largul meu, eram un intrus care nu avea niciun drept să se afle acolo. Președintele și echipa sa dispăruseră, răpiți de bărbații plini de mușchi și cu fețe aspre, în haine de un albastru-închis și în mașini blindate. Bush fusese dus, pe un traseu ocolit, în Omaha, Nebraska, unde era ținut sub protecție în Baza Forțelor Aeriene Offutt, sediul central al Comenzii Strategice. Acest centru de decizie supersecurizat fusese creat în timpul Războiului Rece. În eventualitatea unui atac cu rachete din URSS, de aici președintele ar fi preluat controlul asupra Comenzii Strategice a Forțelor Aeriene și ar fi purtat un război nuclear. Ceilalți guvernanți erau distribuiți în unitățile de înaltă securitate, rezistente la bombardamente, din Maryland, Pennsylvania, Virginia, West Virginia (în locuințe subterane luxoase, în apropierea vechiului club de golf al lui Sam Snead, The Greenbrier) și New England.

Aparent, restul națiunii trebuia să-și înfrunte singură soarta. Eu m-am trezit, în aeroportul din Pittsburgh, în fața unei cozi uriașe. Era alcătuită în cea mai mare parte din cetățeni americani disperați să se întoarcă în New York – sau oriunde altundeva își aveau domiciliul – și străini de pretutindeni, disperați, dimpotrivă, să părăsească țara. Cozile erau vegheate de bărbați gigantici și femei cu chipul împietrit-persoane însărcinate să rezolve rapid orice revoltă. Oamenii așteptau ore întregi, nemișcați și tăcuți, demoralizați și înfricoșați, expuși pentru prima dată ororilor unui atac pe pământ american. În sfârșit, pasagerilor li s-a permis să se împrăstie către destinațiile lor, atunci când a devenit clar că, în pofida amenințării teroriste, traficul aerian trebuia cumva să continue, iar țara începea să se îndrepte cu pași siguri către o fundătură (exact scopul pe care Al Qaeda sperase să-l atingă). Impactul terorii asupra Statelor Unite era groaznic de privit și din el s-a născut o atitudine de intoleranță impasibilă care persistă și azi. Când s-au mai liniștit puțin apele, președintele a ieșit din gaura sa zăvorâtă, iar jalea după morții

din turnurile gemene s-a preschimbat în furie. Uriașul adormit se trezise și a descoperit că informațiile și cunoștințele despre dușman erau dureros de insuficiente.

Comunitatea spionilor americani, așa cum se prezintă ea azi, își are rădăcinile în Pearl Harbor. Americanii știau de atacul japonez, însă informațiile în acest sens se aflau în locuri diferite și erau „proprietatea” unor diverse grupuri militare și civile. Nicio agenție de informații în funcțiune nu avea dreptul de a analiza materialul și de a trage concluzia evidentă. Așa s-a născut Agenția Centrală de Informații (CIA), împărțită în două mari direcții: Direcția Operații, care colectează informațiile, și Direcția Informații, care le analizează. Pare logic, nu? Din nefericire, nu e chiar așa. Din 1946 încoace, au început să se dezvolte alte câteva zeci de colectori de informații. Agenția Națională de Securitate (NSA), care beneficiază de un buget mult mai mare decât cel al CIA, este responsabilă cu interceptarea transmisiunilor, cum ar fi convorbirile pe telefoane mobile și semnalele radio. Vine apoi Biroul Național de Recunoaștere. Treaba lui este să adune informații vizuale de la avioane strategice de recunoaștere și de la sateliții NSA, pentru a le oferi apoi Agenției Naționale de Informații Geospațiale (NGA). Armata și CIA includ, de asemenea, agenții de colectare a imaginilor. Pentagonul răspunde de Agenția de Informații pentru Apărare (DIA), cu propriul serviciu de informații – Servicii pentru Apărarea Umană, care, în același timp, primește informații de la CIA, NSA și NGA. DIA are sarcina de a se concentra asupra capacităților militare ale inamicului – ceea ce nu este deloc ușor atunci când ai de-a face cu o organizație nestructurată și obscură precum Al Qaeda. În plus, toate forțele armate au în subordine propriile agenții de colectare a informațiilor, preocupate în special cu chestiuni tactice, dar care adună întâmplător tot felul de alte materiale.

Mai există și o serie de organizații polițienești civile care activează în domeniul colectării de informații. Biroul Federal de Investigații (FBI) se ocupă atât de contraspionaj, cât și de impunerea legii, având și o responsabilitate contrateroristă.

Acest ultim rol al FBI prezintă o importantă contradicție. Biroul are ca angajați polițiști a căror meserie este aceea de a rezolva infracțiuni comise deja. De fapt, activitatea Biroului este evaluată după rapoartele sale cu infracțiuni soluționate. Contraterorismul se ocupă însă cu împiedicarea producerii unor acte criminale în viitor: colectezi informații, le analizezi și le prevezi efectele. Alte agenții, precum Departamentul Alcool, Tutun și Arme de Foc (AFT), Administrația Antidroguri (DEA) sau Vămi și Siguranța Granițelor (CBS), colectează toate informații, folosite pentru a înlesni arestările și punerile sub acuzare. Departamentul de Stat răspunde de Serviciul de Securitate Diplomatică (DSS), o agenție de contrainformații însărcinată cu protecția ambasadelor SUA. Departamentul Apărării conduce Biroul pentru Planuri Speciale (OSP). Acest grup elitist al „umbrelor” este restrâns, dar puternic, și deține resurse considerabile. Este alcătuit din analiști reputați și obține informații prin secretarul apărării. OSP și desele sale opinii piezișe au primit mai multă atenție decât orice alt grup după evenimentele din 11 septembrie.

Se poate spune că, în 2001, cantitatea de informații deținute de organizațiile militare, de stat și civile din Statele Unite scăpase de sub control, iar analiza acestor informații se apropia vertiginos de un dezastru. Nu exista o singură unitate pe teritoriul Statelor Unite în care să fie colectate, analizate și evaluate toate informațiile obținute de agenții. După tragedia de la turnurile gemene, a devenit imediat evident că excelenta idee a creării CIA după Pearl Harbor fusese de mult abandonată. Diversele interese particulare preluaseră controlul și „comunitatea informațională” se dovedea din nou un haos, în care agențiile concurente scormoneau cu disperare după informații, pe care le păstrau numai pentru uzul propriu. Cunoștințele existau, la fel cum existau motivația, abnegația și tehnologia. În aceste condiții, cum a fost posibil ca 19 teroriști arabi să trăiască, să se instruiască și să acționeze pe tărâmul libertății, pentru ca apoi să deturneze patru avioane și să producă efecte atât de catastrofale?

Ca nou director al Departamentului Național de Informații,

John Negroponte avea la dispoziție un buget de 40 de miliarde de dolari. El avea sarcina de a administra și de a armoniza activitatea celor 15 agenții de informații finanțate de către stat care operează în Statele Unite și de a întreține contacte strânse cu agențiile străine, în special cu cele britanice. Responsabilitățile sale au fost smulse din strânsoarea fostului secretar al apărării, Donald Rumsfeld. Negroponte, diplomat de carieră cu o experiență redusă în lumea informațiilor, a devenit unul dintre cei mai puternici oameni din America și misiunea lui era de a-și folosi abilitățile diplomatice ca să-i forțeze și să-i amăgească pe spionii americani să coopereze, să-i încurajeze să nu se mai întrecă între ei, ci să lucreze împreună pentru binele națiunii. Nu era deloc o misiune ușoară căci serviciile secrete americane, militare și civile – care au fost criticate aspru de către mass-media, politicieni și opinia publică după 11 septembrie, în special cu referire la Războiul din Irak –, riscau să nu-și mai revină niciodată. Trei alte persoane importante au fost contactate înainte ca el să accepte funcția, dar toate au refuzat oferta.

Negroponte s-a născut la Londra în 1939, ca fiu al unei englezoaice și al unui magnat grec din industria navigației. A crescut în Europa, dar a fost educat în New York, unde s-a stabilit familia sa după război. Și-a încheiat educația absolvind Dreptul la Harvard, iar în 1960 a intrat în corpul diplomatic. A doua sa mutare în interes de serviciu a fost ca ofițer politic în Vietnam – „o experiență care îți decide cariera”, cum spunea el. Unul dintre evenimentele de care cu siguranță își aduce aminte este Programul Phoenix, condus de Bill Colby de la biroul CIA din Saigon. O campanie murdară, în care trupele de asasini ai CIA au fost folosite pentru a întemnița, intimida și ucide membri ai guvernului condus de comuniști, constituit de Viet Cong în sudul rural al țării. Programul Phoenix a dus la moartea multor mii de vietnamezi inocenți, iar mișcarea pacifistă a împânzit Washingtonul cu afișe în care Colby era acuzat de crimă. În anii 1980, Negroponte a fost numit ambasador al Statelor Unite în



Honduras, în timpul administrației Reagan, pentru ca apoi să fie acuzat că a închis ochii în fața unor încălcări ale drepturilor omului comise de către CIA. Aceasta i-a ajutat pe rebelii Contras să răstoarne regimul Sandinista, orientat către stânga, din Nicaragua vecină. Au apărut speculații conform cărora el ar fi știut totul și ar fi tolerat „echipele morții” și Batalionul 136, o unitate militară criminală, condusă de Gustavo Álvarez Martínez, general rebel din Nicaragua, precum și că americanii ar fi cooperat la asasinat și torturi. Negroponte a negat toate acuzațiile care i-au fost aduse în mass-media din America. Însă, din când în când, aceste acuzații continuă să iasă la iveală. De-a lungul anilor petrecuți în America Centrală, el a adoptat cinci copii orfani din Honduras, declarând: „I-am luat sub aripa mea, deoarece ei mă vor menține tânăr. Am decis să ne adoptăm toți copiii din aceeași țară, pentru că viața este și așa destul de complicată; nu e nevoie să o îngreunăm cu frați și surori din toată lumea”.

Cariera sa diplomatică l-a purtat prin Orientul Mijlociu, Europa și sud-estul Asiei și a învățat să vorbească fluent limbile spaniolă, greacă, franceză și vietnameză. Ultimul pas în această carieră diplomatică agitată a fost postul de ambasador în Bagdad, unde a fost trimis pentru a-l înlocui pe proconsulul american Paul Bremer. Totuși, se pare că latura sa dură s-a mai domolit, iar activitatea sa în această țară a fost un model de precizie în diplomatie. Acum nu mai este văzut ca un „vultur”, ci ca un funcționar de încredere al statului, cu o reputație de om care tace și face. Susținătorul său la Washington este Colin Powell.

Printre alte agenții, Negroponte controla CIA și FBI; el avea nevoie să-și utilizeze toate abilitățile diplomatice pentru a forma alianțe între cele două. Unul dintre programele cele mai delicate pe care el trebuia să le supravegheze era CAPPSII, un program de scanare a pasagerilor inițiat imediat după atacurile asupra turnurilor gemene – atât de sensibil și de secret, încât, în timpul alegerilor prezidențiale din 2004, a trebuit să fie abandonat discret și temporar. Obiectivul CAPPSII, așa cum a fost descris de nou-înființatul

Departament al Securității Interne, era acela de a crea „un sistem automatic capabil să integreze și să analizeze simultan numeroase baze de date venite de la guvern, industria de informații și sectorul privat, un sistem care să stabilească nivelul de risc estimat pentru fiecare avion de transport, pasager, aeroport și zbor”. Altfel spus, o tentativă de a prezice și de a împiedica potențialii teroriști, folosind toate informațiile pe care Departamentul și agențiile sale pot pune mâna.

Mulți turiști care au avut scurte treceri prin Statele Unite în ultimii ani cunosc procedurile neplăcute necesare pentru a depăși ghișeul de Imigrare. Procesul tinde să fie lent și – în mod deliberat – intimidant: un fel de a ne aduce aminte că, pe tărâmul libertății, mârlandii sunt la putere. La fel ca majoritatea agențiilor, Departamentul Vămi și Siguranța Granițelor își motivează comportamentul de neam-prost, descriindu-l ca „o parte a datoriei noastre vitale de a salva viețile americane”. Sosind recent la aeroportul Kennedy, am fost fascinat de un agent în uniformă și înarmat, înalt, ras în cap și cu privire de oțel, care a apărut în sală în fața maselor ordonate de vizitatori sau turiști și l-a apostrofat cu voce tare pe un tânăr care avusese curajul să-și folosească telefonul mobil în timp ce aștepta să fie evaluat la ghișeu. Așteptasem până atunci mai bine de o oră și am fost obligați să-l ascultăm pe acel oficial urlând abuziv. Era o indicație clară privind disprețul pe care îl avea pentru sărmanii călători. O fată care călătorea cu mine a fost luată într-o cameră din spate și interogată. „Așa mi se întâmplă de fiecare dată când vin aici”, mi-a zis ea când a apărut într-un sfârșit, arătându-mi o scrisoare de la Ambasada Statelor Unite din Londra, în care i se cereau scuze pentru o greșeală apărută în înregistrările călătoriilor ei spre și dinspre America., Angajatorul meu, o companie aeriană, a cerut de zeci de ori ca datele mele să fie corectate, am trimis și scrisori ale unor avocați, dar funcționarii de la Imigrare pur și simplu le ignoră”.

În Marea Britanie, numărul tot mai mare de acte teroriste și violente a coincis cu reducerea dramatică a eficienței forțelor

de poliție și o orientare corespunzătoare, foarte răspândită, către securitatea privată. Când vine vorba despre prevenirea infracțiunilor, poliția noastră este în mare măsură inutilă. Polițiștii sunt dezavantajați de birocrație, de reglementările privind sănătatea și siguranța, de riscul apariției litigiilor, cultura compensației, groaza de a nu fi acuzați de rasism instituțional, un volum imens de noi acte decretate ilegale de către Uniunea Europeană și noua legislație a muncii, precum și de mâna moartă a corectitudinii politice. Moralul lor este mai scăzut ca niciodată, în timp ce povara reclamațiilor care s-au bucurat de succes, legislația drepturilor omului și a protecției datelor întorc șansele împotriva oamenilor legii. Legea protecției datelor din 1998 este împărțită în 75 de secțiuni și prevede pedepse cumplite pentru firmele și indivizii condamnați că nu au respectat-o. Fiecare încălcare a acestei legi poate aduce o amendă de 5.000 de lire sterline. Ea nu a fost niciodată testată adecvat în tribunale și metodele prin care trebuie să fie aplicată nu sunt prea clare.

Filmarea în secret a unui individ, fără înștiințarea sa, este ilegală, iar materialele și informațiile obținute pe această cale nu sunt acceptate ca dovezi în instanță. Unitățile de poliție apelează la firme de securitate private pentru a se proteja împotriva crimei organizate, la fel ca forțele armate, Departamentul Vamă și Accize, cele mai multe ministere (inclusiv cel al Apărării), băncile și toate instituțiile financiare. Poliția britanică, în viziunea omologilor săi continentali, a degenerat într-una dintre cele mai ineficiente forțe de poliție din Europa, dacă nu chiar din lume, în timp ce tehnologiile dezvoltate și comercializate prin industria britanică a securității sunt de cea mai înaltă clasă.

Forțele de poliție și agențiile de securitate folosesc în mod cumpătat supravegherea îndeaproape, deoarece e foarte costisitoare și necesită multe resurse umane. O divizie foarte bine antrenată, ale cărei servicii sunt disponibile atât pentru poliție, cât și pentru serviciile secrete, și care este identificată doar ca S023, oferă supraveghere amănunțită, cu aprobarea unui ofițer superior și, în unele cazuri, a unui funcționar de

stat sau ministerial. Organizația de poliție CIB, cu sediul în Vauxhall (sudul Londrei), este însărcinată cu protejarea apărătorilor legii. Ea beneficiază de fonduri aproape nelimitate, cu care să nimicească orice urmă de corupție din forțele de poliție. CIB are ca angajați ofițeri de poliție deseori refractari, cunoscuți ca incoruptibili, dar îngrijorați de posibilitatea ca nu cumva colegii lor să afle pentru cine lucrează de fapt.

Jocheul Jamie Osborne, după ce a fost arestat sub suspiciunea de a fi aranjat niște curse, a fost abordat de un fost ofițer al Departamentului de Investigații Criminale (CID) din Thames Valley, Robert Harrington, care i-a spus că ar putea face ca investigația asupra sa să fie oprită, fără a i se mai aduce vreo acuzație. Osborne s-a dus direct la poliție și a fost recrutat de CIB ca *agentorovocateur*, în încercarea de a-l prinde în capcană pe Harrington. În ziua anterioară vizitei lui Harrington la Osborne acasă, SO23 instalase un cordon polițienesc în jurul căsuței jocheului și a grădinii sale cu copaci, apoi începuse să instaleze dispozitive de ascultare și camere de filmat atât în locuință, cât și pe teren. Ofițeri bine instruiți erau camuflați și ascunși în grădină, pentru protecție în fața oricărei posibile amenințări la adresa lui Osborne și a altor potențiali martori. Am avut ocazia să ascult casetele și să văd filmul înregistrat – dovezi folosite în procesul intentat lui Harrington și desfășurat la Old Bailey, Curtea Penală Centrală, unde inculpatul a fost condamnat și trimis la închisoare. Camere cu lentile din fibră optică și microfoane au fost ascunse în șemineul din sufragerie și în bucătăria locuinței, iar dispozitive au fost camuflate prin grădină. Locul a fost evacuat și apoi înconjurat cu un cordon polițienesc când au sosit experții în supraveghere; la fel s-a întâmplat după aceea, când ei s-au reîntors pentru a demonta echipamentul. Harrington a mai fost înregistrat în mai multe locuri, folosindu-se numeroase resurse umane și electronice, însă transcrierile convorbirilor și înregistrările întâlnirilor sale cu jocheul au jucat un rol crucial în condamnarea sa.

Au crescut semnificativ numărul agențiilor internaționale

de informații de proporții reduse și private, precum și cererea de companii mici și discrete, precum Hakluyt, înființată de fostul angajat al MI6 Christopher James, ale cărui cunoștințe cu privire la țările în curs de dezvoltare și lumea a treia sunt legendare și care este expert în cine deține puterea în orice țară din lume și în cum poți să-ți înființezi o firmă în locuri dificile de pe planetă. Hakluyt cultivă o „aură” temerară la agenții săi, are un consiliu director înțesat de foști ofițeri de teren și un personal de tineri agenți care operează în cele mai periculoase colțuri de pe glob, unde chiar și cel mai îndrăzneț afacerist s-ar simți nesigur. Stratfor, o agenție globală de informații înființată de George Friedman, este cunoscută în Statele Unite drept „CIA-ul din umbră”, deoarece combină rapoartele și analizele media cu consultanța de spionaj. Ea este, în esență, o vastă rețea colectoare de informații și a ajuns să aibă o influență puternică în comunitatea mondială de spionaj după 9/11, grație analizei sale pătrunzătoare asupra lipsurilor serviciilor secrete americane.

Securitatea privată a înflorit în mare parte ca răspuns la cererile industriei de asigurări că ai lor clienți să se protejeze singuri de spargerii, furturi și violență. Industria de asigurări este capabilă să insiste ca riscurile pe care și le asumă să fie acoperite de un nivel adecvat de măsuri preventive. Se știe că tehnici de supraveghere sofisticate și finanțele necesare sunt disponibile în industria securității de înaltă tehnologie, aflată în continuă dezvoltare. Profiturile sunt imense, iar industria nu este zăpăcită de problemele procedurale și bugetare cu care se confruntă poliția. Industria de securitate a devenit astfel competitivă și inovatoare; ea înfloarește, din moment ce operează profitabil nu doar în protecția sectorului privat, ci și în păzirea instituțiilor statului. Consecința a fost stimularea companiilor de securitate. Organizații precum Kroll, Control Risks și Hakluyt s-au extins, astfel încât să opereze cu succes în comunitatea globală a agențiilor de informații.

Kroll International este o agenție de detectivi specializată în supraveghere electronică și spionaj, condusă din New York de Jules Kroll. Compania operează în 20 de țări, iar personalul

său include aproape 20.000 de specialiști. Filialele internaționale ale Kroll lucrează pentru guverne precum cele din Thailanda și Africa de Sud. De exemplu, compania a sprijinit înființarea Scorpionilor, o forță de securitate internă creată de Nelson Mandela, fostul președinte al Africii de Sud. Serviciile Kroll sunt căutate de afaceri care necesită sfaturi de spionaj și forță fizică pentru a opera pe piețe internaționale dificile. Kroll este probabil cea mai mare și mai sofisticată agenție de acest gen și și-a clădit reputația că este pricepută la depistarea comorilor ascunse ale politicienilor corupți și ale organizațiilor criminale internaționale. Serviciile sale sunt costisitoare. Compania britanică denumită Control Risks, cu sediul pe Victoria Street din City și înființată de compania turistică Hogg Robinson în 1975, oferă consultanță în probleme de securitate corporatistă. Director este generalul Sir Michael Rose, iar agenția sa este specializată în evitarea răpirilor și asasinatelor, precum și în trierea candidaților la un post. Control Risks are 400 de angajați în întreaga lume și o strânsă colaborare cu agențiile de securitate din Marea Britanie, pentru a proteja interesele comerciale naționale.

Pe lângă serviciile de securitate intensivă cu efectiv specializat, care operează mai ales „la sol”, guvernele din întreaga lume au început, după 9/11, să aloce bugete uriașe pentru monitorizarea și interceptarea comunicațiilor electronice. În Statele Unite, interceptarea și interpretarea semnalelor de către Departamentul Justiției, FBI și Administrația Antidroguri își fac simțită prezența în toate formele de sisteme comunicaționale, incluzând acum accesul la internet de bandă largă și telefonie prin Voice Over IP (VOIP). Cetățenii care pălăvrăgesc la telefon, navighează pe internet sau se angajează în tranzacții Online obișnuite lasă în urma lor, fără să-și dea seama, o dâră de detalii personale care sunt automat capturate și reținute în Jurnalele” computerelor. Tehnologia care face posibil acest lucru e într-adevăr uimitoare și poate apărea în cele mai neașteptate locuri.

Baza militară Menwith Hill din North Yorkshire stă sub auspiciile Agenției Naționale de Securitate (NSA) și nu emite

nicio pretenție la vizibilitate sau publicitate. Activitatea sa este fără rețineri neprietenoasă, răspunzând doar în Fața președintelui Statelor Unite și a consilierilor săi pe probleme de securitate națională. Menwith Hill reprezintă interfața dintre Armata americană și spionajul purtat din spațiu, fiind capabilă să intercepteze orice semnal sau conversație din Europa, Africa de Nord și Asia de Vest. Cu cât afli mai multe despre stația de la Menwith Hill, cu atât te enervezi mai tare. Ea reprezintă o piesă importantă de armament de război, ascunsă în nordul Angliei, și unul dintre locurile cele mai secrete de pe glob. Fără cel mai înalt nivel posibil de transparență, nimănui nu îi este permis accesul dincolo de porți. Americanii nici măcar nu recunosc că stația există și refuză să lase orice vizitatori, inclusiv membri ai Parlamentului național sau ai Parlamentului European, să intre aici, chiar și în ocazii oficiale. Alice Mahon, membră a Parlamentului din partea laburiștilor, a spus în fața camerelor că nicio persoană preocupată de libertățile cetățenești nu poate ignora Menwith Hill. În pofida numeroaselor tentative de a primi răspunsuri la întrebările ei, este evident că baza militară nu răspunde în fața membrilor Parlamentului britanic și, ca atare, nici în fața poporului britanic. Deși este o stație de supraveghere americană, în 1996 ea a fost inclusă, prin denumire, în Forțele Aeriene ale Marii Britanii, în încercarea de a camufla ce reprezintă această puternică resursă militară. Oricum, ea nu este singura în această situație: există stații similare, chiar dacă mai mici, în Australia și Austria.

Baza militară este imposibil de ascuns, nu o poți îngropa sau muta sub pământ. O zărești la orizont atunci când lași în urmă Harrogate pe autostrada 59 și pătrunzi în Yorkshire. De la distanță, pare o colecție de „cupole” emisferice, mari și albe, așezate în ceea ce fusese odinioară o liniștită regiune necultivată. Domurile conțin „farfurii” de recepție a informațiilor transmise de sateliți și sunt înconjurate de clădiri „întărite” (rezistente la bombardamente). Menwith Hill este cea mai mare stație de monitorizare electronică din lume și acolo lucrează 1 200 de civili și militari americani.

Administrația Națională pentru Aeronautică și Spațiu (NASA), care controlează baza, a mai angajat un număr limitat de civili britanici, verificați cu atenție, din Sediul Comunicațiilor Guvernamentale (GCHQ). Baza a crescut de-a lungul anilor, iar puterea și importanța de care se bucură sunt subliniate de închiderea celorlalte stații conduse de NSA din Marea Britanie. Noua ei destinație oficială, de Centru Operațional pentru semnale de spionaj (SIGINT), responsabil cu conducerea de la distanță a stațiilor automate de colectare a informațiilor, subliniază importanța strategică a bazei.

Motivul pentru care acest memento fățiș al lumii pline de pericole în care trăim mă calcă pe nervi este faptul că baza interceptează tot „traficul” informațional care intră în, iese din, sau trece prin Marea Britanie și care are ca origine sau destinație Asia de Vest, Africa de Nord și Europa. Baza este de importanță vitală pentru americani, deoarece sateliții poziționați astfel încât să recepționeze comunicațiile din aceste regiuni sunt „vizibili” din Menwith Hill, dar nu și din Statele Unite. „Traficul” include toate apelurile pe telefonul mobil, mesajele pe mobil și prin satelit, e-mailurile, faxurile, semnalele radio și orice alt tip de comunicare electronică cunoscut omului. Dacă un semnal trece printr-un cablu sau printr-un releu radio ori satelit, stația îl poate recepționa, analiza, procesa și retransmite automat către Statele Unite.

Stația de la Menwith Hill a jucat un rol major în invadarea Irakului din 2002, interceptând și transmițând informații de comandă. Războiul a fost purtat de americani în primul rând ca un război spațial, în care aliații puteau folosi 50 de sateliți care să sprijine eforturile militare britanice și americane; 27 de sateliți de poziționare globală au fost utilizați pentru a detecta amplasarea unităților și țintelor operațiunilor speciale, iar restul pentru a transmite comunicații și comenzi și pentru avertismente privind atacuri cu rachete, tipare de condiții meteorologice și multe altele. Generalul Judd Blaisdell, directorul operațiunilor spațiale din cadrul forțelor aeriene americane, a afirmat că în jur de 33 600 de persoane, lucrând în 36 de stații SIGINT din întreaga lume, au fost implicate în



activități de tipul „război spațial”. Supravegherea prin satelit a fost susținută cu date oferite de AWACS (mari aeronave de comunicații ce rătăcesc la „marginea” spațiului) și de spionajul uman.

Sistemele nu erau în niciun caz ireproșabile. Unele rachete Tomahawk și-au ratat cu mult ținta în timpul invadării Irakului, iar lungimea de bandă-radio disponibilă s-a dovedit a fi inadecvată. Ultimul război din Irak a reprezentat o rafinare a tehnicilor utilizate în Războiul din Golf din 1991. Toate bombele și armele inteligente erau controlate de sateliți spațiali de poziționare globală și acum este evident că sistemele spațiale sunt cheia viitoarei puteri militare americane. La sfârșitul acțiunilor militare din Irak, în aprilie 2003, vorbind la inaugurarea celui de-al 614-lea escadron de spionaj spațial, la baza aeriană Vandenberg din California, comandantul locotenent-colonel Earl White a remarcat că folosirea tehnologiei spațiale fusese un avantaj major în război. „Fără spațiu, revenim la al Doilea Război Mondial, a zis el. Oricine vrea să ne înfrunte va trebui să ne înfrunte în spațiu”.

Baza de la Menwith Hill a reprezentat o importantă valoare militară în timpul ambelor războaie împotriva Irakului. Ei îi revine marea responsabilitate de a intercepta și transmite informații de spionaj militar și de comandă, pe lângă funcțiile sale de a obține date sau de a culege și analiza informații de spionaj civil și comercial. Rolul său nu poate decât să crească, pe măsură ce America dezvoltă mai multe sisteme de luptă cu baza în spațiu. Stația de la Menwith Hill acoperă o suprafață de aproximativ 20 de acri și controlează 56 de sateliți dintr-o serie cunoscută drept „The Runway” („Podiumul”), care operează în linie de la est la vest, la extremitatea sudică a bazei. În prezent, baza operează două sisteme: „Silkworth” și „Moonpenny”. Sistemul „Silkworth”, operat dintr-o clădire mare și joasă din centrul bazei, găzduiește o rețea de computere ce monitorizează sateliții staționați deasupra Ecuatorului, unde interceptează transmisiuni radio la distanță mare de la țintele din Eurasia și le retransmit către bază.

Tehnologia permite personalului să asculte mesaje și conversații dintre indivizi și companii din Orientul Mijlociu și Europa. Ele sunt retransmise de sateliții Mercury, Magnum și Orion (mai avansat). Acești sateliți, la fel ca aproape toți sateliții moderni de comunicații, sunt „geosincroni” – asta înseamnă că rămân într-o poziție fixă în raport cu Pământul. Datele sunt descărcate și retrimise pentru analiză în Yorkshire, unde sunt sortate după criterii speciale într-o unitate subterană, protejată împotriva radiațiilor, numită „Steeplebush II”.

Operațiunile speciale „Moonpenny” sau sistemele „Sprinkler” („Stropitoare”) interceptează și recepționează comunicații neautorizate prin satelit din alte țări. Ele constau dintr-o serie de terminale de interceptare, programate să adune semnale de la sateliții de comunicații naționali și internaționali aflați sub controlul altor state (inclusiv „Arabsat” și „Intelsat”). Amploarea procesului de colectare este impresionantă. NSA are ca obiectiv strângerea tuturor comunicațiilor internaționale și a majorității celor naționale. În 1992, sistemul intercepta 2 milioane de mesaje pe oră, dintre care toate, în afară de vreo 13.000, erau ignorate înainte de filtrare până la a se ajunge la cele 2000 care satisfăceau criteriile pentru a fi transmise mai departe. Acestea din urmă erau reduse treptat, rezultând în final 12 comunicații care erau selectate și analizate de experți. Acum 15 ani, stația Menwith Hill intercepta anual 17, 5 miliarde de mesaje, dintre care vreo 17, 5 milioane puteau fi analizate.

Echelon este un sistem global de interceptare, administrat și de NSA, care captează și analizează în principiu orice apel telefonic, fax, e-mail și mesaj telex trimis oriunde în lume. Este operat în colaborare cu GCHQ din Cheltenham, Instituția pentru Securitatea Comunicațiilor (CSE) din Canada, Direcția pentru Apărare și Securitate (DSD) din Australia și Biroul General pentru Securitatea Comunicațiilor (GCSB) din Noua Zeelandă. Aceste organizații sunt reunite printr-un acord din 1948, UKUSA, ale cărui prevederi rămân încă secrete. Potrivit unei investigații a Comisiei Uniunii Europene din 2001,

sistemul Echelon furnizează analiștilor britanici și americani date colectate de 120 de sateliți-spion. Acest lucru înseamnă că, în fiecare minut al fiecărei zile, sistemul poate procesa 3 milioane de comunicații electronice. Proiectul Echelon e simplu; el interceptează stații din întreaga lume. Captează întreg traficul de comunicații prin satelit, microunde, telefoane mobile și fibre optice, apoi procesează informațiile prin intermediul computerelor de la NSA, care includ programe avansate pentru recunoașterea vocii sau recunoașterea optică a caracterelor. Personalul NSA mai caută cuvinte sau fraze de cod (așa-numitul „dicționar” Echelon), care determină computerul să marcheze mesajul, pentru a fi înregistrat și transcris, în vederea unor viitoare analize. Analiștii informațiilor din cadrul fiecăreia dintre respectivele „stații de ascultare” au liste separate de cuvinte, care îi ajută să analizeze conversații sau documente marcate de sistem, iar acestea sunt apoi transmise agenției de informații care a solicitat interceptarea. Se spune că Echelon este folosit și pentru interceptarea supravegheri interne, a civililor americani, pe motive de afiliere politice „nepopulare” sau fără cauze evidente. Dacă e adevărat, atunci este vorba de spionaj politic și sunt violate amendamentele 1, 4 și 5 din Constituția Americii.

Raportul Parlamentului European intitulat „O estimare a tehnologiilor de control politic”, editat de Comitetul pentru Evaluarea Opțiunilor Științifice și Tehnologice din cadrul Parlamentului European, ridică întrebarea dacă interceptarea comunicațiilor de către Echelon nu violează suveranitatea altor state și intimitatea cetățenilor acestora. Nu prea mai există îndoială că stația de la Menwith Hill îi supraveghează pe cetățenii britanici pe teritoriul țării, cu știința și cu întreaga colaborare a guvernului britanic.

Echelon a fost creat cu sprijin de la GCHQ din Cheltenham și, în 1993, elemente nemulțumite din interiorul comunității spionilor britanici au utilizat rețeaua pentru scurgerea unor informații privind încercările americane de a câștiga voturi la Națiunile Unite în favoarea intervenției în Irak. Comunitatea

britanică de spionaj a fost foarte nemulțumită de tentativele guvernului de a deforma informațiile primite susținând că Irakul menținuse contacte cu rețeaua teroristă Al Qaeda. O femeie de 28 de ani, angajată a GCHQ, a fost arestată fiind suspectată de a fi încălcat Legea secretelor de stat. Se credea despre ea că ar fi lăsat să se scurgă un memoriu al NSA în care se solicitau informații din „liniile de produse” (în jargonul SIGINT, asta înseamnă interceptări ale convorbirilor telefonice și e-mailurilor), ordonând un „val” de spionaj îndreptat împotriva țărilor Angola, Camerun, Chile, Bulgaria și Guineea, cu „un accent suplimentar pe problemele Națiunilor Unite legate de Pakistan”. Scris de Frank Coza, șeful personalului de apărare (pentru obiective regionale), memoriul a fost pus în circulație, în același timp, de NSA. Operațiunea, autorizată probabil de Condoleezza Rice, consultant pe probleme de securitate națională, i-ar fi implicat, se pare, și pe Donald Rumsfeld și George Tenet, directorul CIA. Președintele Bush a știut cu siguranță de ea. Scurgerea de informații a fost un act de sfidare atent plănuțit, care a ilustrat nemulțumirea din serviciile secrete privind modul în care britanicii și americanii întrebuințau abuziv spionajul. Ruptura cu „seniorii” din lumea informațiilor se accentuase de ceva timp și nu fusese ameliorată de dezvăluirea că în biroul lui Kofi Annan, secretarul general al ONU, fuseseră plantate microfoane de către americani.

Orice s-ar întâmpla, baza de la Menwith Hill continuă să crească și aproape a dus la bun sfârșit proiectul Sistemului Infraroșu Spațial (ZBIRS), pentru care până și NSA a fost obligată să ceară permisiunea Consiliului Districtual Harrogate înainte de a-l putea instala. Nu există rachete sau alte sisteme aeriene de apărare în această bază, deși nimeni nu se îndoiește că, în eventualitatea puțin probabilă a unui atac nuclear, ea va fi una dintre țintele principale. ZBIRS este doar un alt nume pentru „Războiul Stelelor”. Patru sateliți noi au fost lansați pe orbită pentru a înlocui cele patru vehicule spațiale excedentare din cadrul Programului de sprijin al Apărării. Printre alte progrese, noul sistem poate detecta în

spațiu „corpuri reci”, precum și semnături cu infraroșii de la arderile motoarelor de rachete. Într-un discurs ținut în fața Congresului, generalul american Howell M. Estes DI, șeful Centralei Nord-americane pentru Apărarea Aerospațială, a afirmat că sistemele ZBIRS vor îmbunătăți capacitatea americanilor de a „oferi rachete balistice mai precise ca lansare și punct de impact forțelor aflate într-un teatru de operațiuni militare”. Cu alte cuvinte, acuratețea și ferocitatea puterii de foc americane, care sunt controlate din spațiu, devin tot mai eficiente pe zi ce trece.

Frica și furia induse de secretomania ce înconjoară Menwith Hill au creat, după cum era de așteptat, și revoltă politică. Speculațiile privind activitățile desfășurate de americani pe teritoriul britanic sunt nesfârșite. Europarlamentarii cer în mod regulat să afle exact ceea ce se petrece în baza militară, dacă americanii au primit acces la secrete ale comerțului european (ceea ce, evident, s-a întâmplat) și dacă acest lucru periclitează securitatea europeană. Fără îndoială, e greu de imaginat că americanii ar tolera o unitate britanică sau europeană similară pe teritoriul lor, și la fel de greu e de înțeles de ce această bază NSA nu ar trebui să răspundă în fața guvernului britanic.

Ostilitatea locală față de stația de la Menwith Hill reprezintă mai mult decât o ridicare din umeri ca în Yorkshire și un bombănit „asta nu-i treaba mea, băiete”. Localnicii vor să știe ce se întâmplă dincolo de gardul de sârmă ghimpată și de ce o bază atât de uriașă nu primește forță de muncă indigenă. Puținii tehnicieni și analiști din Cheltenham care staționează acolo reprezintă totalul implicării britanice. Scena din afara bazei aduce aminte de protestele antirăzboinice de la Greenham Common. O prezență constantă este cea a doamnelor trecute prin multe de la sediul local din Yorkshire al Campaniei pentru Dezarmare Nucleară (CND), care stau în corturi și fac ceai la focuri aprinse cu surcele, provenind din foste barăci. Ele stau aici deja de ani buni și acceptă cu seninătate că mai au destul de așteptat. Protestatarii încalcă în mod obișnuit proprietatea, pătrunzând în bază, iar activitățile

lor scot în evidență lipsa generală de umor sau de înțelegere a Armatei americane când vine vorba de asemenea demonstrații. Rezultatul e că, din când în când, se întâmplă ceva care dovedește că până și o unitate destinată războiului poate avea o parte ridicolă.

Atunci când, în 1997, două femei, Helen John și Anne Lee, au făcut apel la condamnarea pentru violarea unei proprietăți la Curtea Regală York, un avocat al British Telecom (BT) a fost chemat ca martor. Acest reprezentant al companiei a lăsat să-i scape informația că BT instalase trei cabluri din fibră optică cu capacitatea de a purta mai mult de 100.000 de apeluri telefonice simultan către baza militară americană. Avocatul, pesemne prost instruit de clientul său, a oferit Curții de Apel detalii despre cabluri, pentru a fi apoi sfătuit de judecător să-și retragă mărturia. Vechea „Poștă Generală” (predecesorul BT) furnizase inițial două circuite cu „lățime de bandă mare”, pentru capacități ridicate, către Menwith Hill în 1975. Acestea erau conectate prin cablu coaxial cu rețeaua BT din Hunters Stones, o stație radio cu frecvență înaltă, aflată aproape de baza americană. În anii 1970 și 1980, aproape toate apelurile telefonice la distanțe mari treceau prin Hunters Stones. BT admitea acum că aceste cabluri erau conectate direct, suboceanic, cu Statele Unite. Cum a afirmat compania în mărturie, capacitatea de transmisie a fost triplată între timp, adăugându-se alte două legături prin fibră optică.

Avocatul BT a mai afirmat că alte companii de telecomunicații britanice au furnizat echipamente de interceptare bazei americane și că aceste companii britanice erau implicate în activitățile de spionaj de la Menwith Hill. Revelațiile datorate avocatului BT au fost întrerupte brusc de intervenția judecătorului, care a acuzat martorul că divulgă secrete naționale. BT a trimis apoi un al doilea avocat, în încercarea de a interzice mărturia. Astfel, recursul s-a transformat într-o farsă, însă un colț al cortinei ce acoperă activitățile de supraveghere britanice a fost ridicat, chiar și pentru scurt timp, pentru a dezvălui că guvernul nostru oferă americanilor nu doar informații militare, ci și secrete

comerciale, prin intermediul unor firme locale. Zi de zi, date furnizate de companii britanice devin disponibile analiștilor de la Menwith Hill.

Sediul Comunicațiilor Guvernamentale (GCHQ), stația de recepție a guvernului din Cheltenham, este descris ca un „luptător împotriva infracționalității” de către Comitetul Reunit de Informații, responsabil pentru el. De fapt, această bază este unul dintre cei mai sofisticați colectori de informații din lume. În 2004, el a fost mutat la periferia Cheltenhamului, unde fusese special construită o stație de recepție în care s-a investit un miliard de lire sterline. Securitatea informației transmise din GCHQ se află în sarcina Grupului de Securitate a Comunicațiilor Electronice (CESG). De interceptarea SICIINT se ocupă Organizația pentru Semnale Complexe, care are birouri în Cheltenham, dar și în Cornwall și pe insula Ascension.

GCHQ furnizează informații tuturor serviciilor de securitate și le împarte cu baza de la Menwith Hill și cu NSA. De fapt, organizația are personal comun cu americanii și utilizează aceleași metode pentru a „semnaliza” informații de la sateliți sau din alte surse electronice în și din Insulele Britanice. GCHQ participă la sistemul american Echelon folosind dicționarul Echelon pentru a captura „produse” – informații de spionaj utile. O bună parte din activitatea GCHQ este limitată la agențiile de informații britanice, însă organizația a fost implicată puternic în pregătirea Războiului din Irak, ceea ce a provocat supărarea multora dintre cei 3.500 de angajați de la Cheltenham – de aici, nemulțumirea și scurgerile de informații.

Această formă de colectare a informațiilor este menită să fie camuflată complet – există prezumția că subiectul „trasului cu urechea” electronic nu este conștient că e spionat; altfel, informațiile acumulate devin inutile. Însă există o modalitate mai directă – și mai nepăsătoare – de a extrage informații de la suspectii de terorism: tortura. Desigur, tortura este ilegală pe teritoriile americane și britanice. Însă, atunci când ești o organizație ce strânge informații care beneficiază de întregul

sprijin al celor mai sus-puși oameni ai țării, se găsește de obicei o cale de a ocoli o problemă minoră precum ilegalitatea. CIA și NSA, desperate după o analiză a amenințării teroriste, au extras liste de informații obținute de la afghani și alți suspecți din Orientul Mijlociu. Administrația cerea rezultate și le dorea rapid. CIA a intensificat folosirea a ceea ce e cunoscut drept „Transfer”. Acest termen este o creație americană deosebit de cinică, susținută fără rușine de britanici. Ceea ce ne interesează aici este Transferul extraordinar”, un eufemism pentru „a te baza pe altcineva pentru a-ți face treburile murdare”.

Această practică, descrisă în termeni reci și detașați, sună ca o povestire scrisă de Franz Kafka în barul unui hotel, chiar înainte de ora închiderii. Ceea ce o face în mod special alarmantă este faptul că guvernul britanic cooperează entuziast, în deplină cunoștință de cauză, la ducerea la îndeplinire a acestei practici. Oficialii americani admit că „Transferul extraordinar” a fost folosit de CIA de cel puțin 200 de ori, ceea ce înseamnă aproape sigur că a fost folosit de mult mai multe ori, dar că această cifră este singura pe care își permit s-o recunoască. Se știe că, în întreaga lume, diferiți indivizi au fost răpiți, hainele lor au fost tăiate cu cuțitele, trupurile-umplute cu sedative, încheieturile mâinilor și picioarele – înlănțuite, fețele – mascate și acoperite cu glugi, corpurile – înfășurate în scutece și îmbrăcate în veșminte portocalii. Precum pachetele de carne, ei au fost transportați în avioane administrative Gulfstream către state precum Egipt, Maroc și Uzbekistan, unde extragerea de informații prin metode precum fierberea brațelor, amenințarea cu aruncarea de pe o scândură în apă, lovirea repetată cu ciocane sau atașarea unor electrozi de organele genitale sunt întâmplări cotidiene. Altfel spus, „Transferul extraordinar” este pur și simplu un eufemism pentru forțarea suspecților de a-și mărturisi implicarea în acte teroriste, prin supunerea lor la torturi. Singurul motiv imaginabil pentru care americanii sunt gata să facă asta este credința lor că scopul scuză mijloacele. Ei sunt convinși că acei oameni sunt teroriști militanți și că,



din moment ce organizațiile de impunere a legii sunt restricționate de reguli procedurale stricte în țările lor, ei nu dispun de mijloacele legale de a-și supune suspectii nivelului de presiune fizică și emoțională necesar pentru a-i forța rapid să vorbească.

Calitatea informațiilor obținute prin tortură fizică și mentală este recunoscută ca inferioară. Am discutat despre asta cu un ofițer din Divizia Specială, cu o experiență îndelungată în interogarea suspectilor IRA; el a comentat: „Poți convinge pe cineva să spună orice, dându-i speranța că vei înceta să-i mai provoci durere. Asta nu înseamnă că spune adevărul”. Și a continuat: „Există metode mai rapide și mult mai eficiente de a obține același lucru. Tortura pur și simplu nu funcționează ca mijloc de obținere a unor informații semnificative”. Motivația care îi determină pe americani să recurgă la asemenea acțiuni sălbatice și nejustificate este dublă. În primul rând, procesul legal în Statele Unite este interminabil și scrupulos, cu procese de apel întinse și referiri constante la drepturile omului. Sistemul penal american este recunoscut drept brutal, însă numai pentru aceia condamnați pentru infracțiuni. Golful Guantánamo din Cuba găzduiește suspecti fără reprezentanți legali, care pot fi tratați ca neavând drepturi cetățenești. Atât cât este implicată administrația Bush, teroriștii nu sunt protejați de Convenția de la Geneva, dar, pentru a evita stânjeneala, suspectii sunt ținuti departe de patrie și de orice posibilitate de obstacol legislativ, fiind întemnițați în unități secrete, controlate de CIA, din întreaga lume. Agențiile de securitate americane implicate sunt judecate după rezultate, iar o mărturisire, chiar și sub constrângere, echivalează cu un bonus. De asemenea, teama de a fi capturat și transferat în secret într-o celulă subterană, în barăcile secrete din Cairo, îl va preocupa chiar și pe cel mai înfocat „luptător pentru libertate”, iar zvonurile despre ororile care așteaptă pe oricine e suspectat de CIA s-au răspândit rapid în întreaga lume arabă: în 2005, George W. Bush a fost întrebat, la o conferință de presă de la Casa Albă, despre practica „Transfer extraordinar”, la care recurg agenții CIA.

Președintele a ezitat să răspundă, a examinat podeaua, a făcut o pauză, și-a aruncat privirea prin încăpere, a tușit, apoi a șoptit că practica există, dar este justificată, deoarece „este o măsură antiteroristă și nu există nimic ce nu aș face pentru a împiedica moartea cetățenilor americani”. Cu două luni mai devreme, pe 27 ianuarie, într-un interviu pentru *New York Times*, Bush declarase: „Tortura nu este niciodată acceptabilă. Noi nu trimitem niciodată oameni în țări care practică tortura”. Aceasta a fost o minciună sfruntată.

Există, din păcate, prea multe dovezi privind practicarea „Transferului extraordinar” pentru a ne mai îndoi că această practică are loc. Mai rău e că, prin recurgerea la asemenea metode extreme, Statele Unite își trag la fund și prietenii, și aliații. Avioanele utilizate și operate de CIA, sub numele de cod „Transport administrativ prioritar”, își fac plinul în mod regulat în baze ale Forțelor Aeriene Regale și în aeroporturi civile din Marea Britanie, iar informațiile obținute prin tortură ajung la analiștii de spionaj britanici, care le examinează cu sânge rece. Principala problemă pe care o au de înfruntat echipajele de navigație și asasini cunoscuți ca „Unitatea Specială de Evacuare”, care efectuează aceste transferuri în timpul programului lor de zbor în jurul lumii, a fost, dintre toate, marele amator de aviație britanic. Această pasiune puțin cam aiurită s-a transformat într-o rețea de membri largă și foarte eficientă. Un avion Gulfstream cu numărul de înregistrare N379P a fost asociat de ei cu o firmă de chartere numită „Premier Executive Travel”, o companie-fantomă cu sediul în biroul unor avocați de la periferia Massachusetts-ului și un președinte cu o adresă înregistrată în Arlington, Virginia, aproape de sediul CIA. Avionul a fost observat în mod regulat făcând curse în spațiul aerian britanic; se știe că a aterizat la Brize Norton, Mildenhall, RAF Leuchars, Luton și Glasgow. Intrările în și ieșirile din Marea Britanie i-au fost notate cu mare sârguință de către detectorii de avioane și înregistrate în bazele lor de date, potrivit lui Chris Yeats, un expert în operațiuni aeriene. Avionul a fost prezent de atâtea ori aici fie pentru a-și face plinul, fie pentru a lua parte la procesul de

„Transfer” din Marea Britanie către medii mai puțin blânde din Africa și Orientul Mijlociu. Agențiile de spionaj americane utilizează în mod obișnuit avioane ale unor companii particulare pentru operațiile lor, cu scopul de a distra atenția de care au parte în general avioanele militare. Oricum, CIA a greșit neluându-i în calcul pe pasionații de aviație britanici.

Odată ce ziariștii au descoperit că o companie de aviație privată sprijinea CIA și au început să pună întrebări incomode, sediul firmei Premier Executive Travel și detaliile sale de înregistrare au fost imediat modificate. Se știe că avioane particulare având la bord agenți CIA au aterizat și pe aerodromul Bromma din Suedia, unde forțele speciale de intervenție au ridicat doi egipteni de pe o stradă lăturalnică din Stockholm. Cei doi erau suspectați de asocieri cu Al Qaeda și au fost ținuți în Suedia timp de opt ore, înainte de a fi sedați și transportați cu avionul la Cairo, unde au fost închiși și supuși timp de câteva luni la torturi și interogatorii. Unul din ei, doctorul Aziza, a reușit să dea un telefon soției sale Hanna înainte de a fi drogat de Unitatea Specială de Evacuare. Doctorul Susan Fayed, lucrător medical la Nadim, un refugiu solitar egiptean și un centru de reabilitare pentru victime ale torturii, mi-a spus că primesc persoane care au fost ținute în închisoare și eliberate cu fracturi, arsuri și paralizie provocate de tortura cu electricitate. Ea afirmă că doctorul Aziza a fost vizitat de mama sa, după ce torturile începuseră să își facă efectul, și se afla în stare șocantă. Ulterior, el a fost condamnat la 25 de ani de muncă silnică. Tovarășul său a fost eliberat și este arestat la domiciliu în Cairo; e prea îngrozit pentru a vorbi despre experiențele sale. „Americani știu ce se petrece acolo, spune doctorul Fayed. Multe dintre victimele pe care le-am văzut la centrul Nadim au fost aduse aici de Unitatea Specială de Evacuare”.

Craig Murray, ambasadorul Marii Britanii în Uzbekistan (o mică și urâtă dictatură, înghesuită între Afghanistan și Rusia), a realizat că este urmărit atunci când a fost invitat la cină de profesorul Jamal Mirsaidov, un militant pentru drepturile,

omului din Taşkent. A doua zi, nepotul lui Mirsaidov a fost găsit torturat până la moarte. Fusesse bătut cu bare de fier și apoi fiert de viu. Autoritățile uzbece au pretins că de fapt căzuse victimă unei supradoze. Murray a devenit îngrijorat atunci când a descoperit, dintr-o conversație cu un agent MI6, că serviciile de securitate britanice considerau că informațiile transmise din Uzbekistan către CIA și MI6 erau de cea mai înaltă calitate și încredere. El a revenit la Londra în 2003, pentru a protesta în fața superiorilor săi din Ministerul de Externe, care primiseră consultanță legală de la unul dintre magistrații lor, un anume M.C. Wood. Acesta a confirmat că este legal „să deții informații obținute prin tortură”. Murray a discutat cu Jack Straw, ministrul de externe, care i-a declarat că, deși are „nopti nedormite din cauza asta”, trebuie să urmeze sfatul serviciilor de spionaj.

Lăsând deoparte implicațiile morale ale actualei forme de colectare a informațiilor, în care totul este permis, consider că serviciile de securitate americane și britanice sunt vulnerabile la farse și greșeli, cum se întâmplă peste tot. Acest lucru este valabil mai ales în cazul supravegherii. „Spionilor” le place să spună că doar eșecurile și erorile se află, pentru că restul e secret. Așa o fi, dar cum putem noi ști asta? Un exemplu faimos: americanii n-au reușit să prevadă atacurile Al Qaeda asupra World Trade Center, în pofida faptului că Osama Bin Laden mai încercase o dată să distrugă clădirea, punând un om al său să planteze un camion-bombă în subsolul ei. De fapt, eșecurile spionilor americani și britanici au o istorie mult mai lungă. Serviciile secrete americane nu au ratat doar Pearl Harbor, ci și căderea Zidului Berlinului, și n-au avut habar de decizia lui Hrușciiov de a trimite rachete în Cuba până când armele nu au fost fotografiate *en route* de un avion-spion U2. Spionii britanici nu au reușit să prevadă închiderea Canalului de Suez de către președintele Egiptului, Gamal Abdel Nasser, care a generat o criză în 1956. Ei au fost prinși nepregătiți de începerea campaniei cu bombe a IRA, de căderea șahului Iranului sau de invadarea insulelor Falkland de către Argentina. Când e vorba de aflarea unor detalii precum locul

unde își ascunde Mugabe milioanele strânse din jafuri sau sub ce acoperiș își cultivă marfa un traficant de droguri, avem cu siguranță cunoștințele și capacitatea de a afla adevărul. Mai știm și multe lucruri privind obiceiurile și slăbiciunile subiecților noștri, deoarece – cum am văzut deja – suntem de departe cea mai supravegheată țară din lume. Însă, atunci când vine vorba despre predicțiile amănunțite și analiza marilor evenimente, se pare că nu dispunem de competența de a cerne informațiile, de a le examina amănunțit și de a pune planuri la cale, iar americanii stau la fel de prost ca noi.

Incapacitatea de a prevedea marile evenimente, în ciuda informațiilor deținute de agențiile ce operează în numele statului, se datorează cu precădere incapacității de a analiza ce s-a aflat până acum prin spionaj, mai ales din pricina calității personalului angajat de serviciile de securitate și a „factorului uman”, supus greșelii. Toate marile puteri sunt mai preocupate să acumuleze informații decât să le analizeze. Lipsa unei unități, a unei clarități a scopului și a unei viziuni de ansamblu a diverselor agenții de informații creează erori politice deseori catastrofale, care ies la iveală după evenimente. Misiunea oficială a CIA este aceea de a furniza informații externe exacte, bazate pe dovezi, cuprinzătoare și de actualitate privind securitatea națională, precum și de a desfășura activități de contraspionaj, activități speciale și alte funcții asociate cu informațiile externe și securitatea națională, la ordinul președintelui. Dacă obiectivul este ca informațiile să fie bazate pe probe, cine stabilește parametrii? Și de ce nivel al dovezilor este nevoie pentru a justifica „activitățile speciale”? Desigur, se prea poate ca această declarație să fi fost redactată de un omuleț în pantaloni de bumbac bej, locuind pe Madison Avenue, căruia sintagma „activități speciale” i-a atras atenția și i-a provocat un fior. Nu se știe niciodată.

În schimb, știm că bugetul anual al comunității agențiilor de informații din SUA este de 40 de miliarde de dolari, deși se pare că încă le mai scapă subiectele mari. La fel ni se întâmplă și nouă. Chestiunea rateurilor serviciilor secrete va fi abordată

mai detaliat în capitolul IX.

## Capitolul VII

### Ochiul din cer

*Avem cu toții o vagă idee despre niște piese metalice sofisticate numite sateliți, care orbitează deasupra capetelor noastre; credem că sunt, în general, un lucru bun. Ei nu sunt utilizați doar pentru a explora spațiul cosmic, dar ne aduc televiziuni din întreaga lume și sprijină sisteme de radionavigație prin satelit (GPS) sau resurse puternice pentru telefonie mobilă. Ei observă vremea și pot urmări chiar și evoluția furtunilor de nisip din Africa de Nord. Sateliții mai sunt folosiți pentru a trasa mișcările globale ale peștilor și animalelor; de exemplu, chinezii utilizează supravegherea prin satelit ca să monitorizeze obiceiurile de migrație ale populației sale de 4.000 de cocori cu gâtul negru. Uniunea Europeană verifică dacă terenurile nelucrate pentru care fermierii primesc beneficii nu sunt cultivate, iar extinderea incendiilor forestiere este urmărită pe întreg globul, de la arhipelagul grecesc până la Amazon.*

Supravegherea prin satelit a fost foarte eficientă în stăvilirea poluării cu petrol cauzate de practica – foarte răspândită odinioară – a navelor comerciale de a-și goli rezervoarele de petrol în larg. În 2005, se aflau pe orbită 31 de sateliți, ce ofereau imagini ale suprafeței terestre, cu rezoluții similare fotografiilor făcute de la 1 la 30 de metri. Dintre acești sateliți, 14 sunt finanțați privat de corporații americane, fiecare dintre ei având imagini cu rezoluții corespunzătoare la cel mult zece metri. Sistemele ieftine de sateliți comerciali, care devin operaționale în prezent, oferă imagini cu rezoluții chiar și mai bune, iar ei vor deveni o parte importantă a marketingului orientat către consumatori,

fiind utilizate pentru a monitoriza traseul mărfurilor pe întreg globul. Însă nu este oare deranjant să ne gândim la „atotștiutorul ochi din cer”, care poate alege din mulțime pe oricine dintre noi și să-l urmărească pretutindeni, atât cât are el chef? Cum ne putem proteja intimitatea de asemenea sisteme îndepărtate, dar foarte eficiente, care operează într-un spațiu ce nu se supune normelor legii sau votului democratic? Țări din întreaga lume – și mai ales Statele Unite – cheltuiesc sume imense pentru a face cât mai mici tehnologiile ce le permit să-și bage nasul peste tot. Drept rezultat, camera-spion nu trebuie să fie pe orbită, în spațiu, pentru a vedea ce faci; ea poate pluti într-un colț al încăperii tale.

Dintre toate sistemele de spionaj, ce mă supără cel mai mult este gândul că pot fi urmărit de sateliți. Nu e suficient de rău că sunt camere de supraveghere pe străzi și în magazine, că trebuie să completez formulare intruzive pentru agenții guvernamentale precum Administrația Financiară și să-mi dovedesc identitatea de fiecare dată când ajung, în concediu, pe aeroportul Kennedy, acum mai trebuie să fiu conștient și de un fapt menit să-mi distrugă nervii: un lucru invizibil din spațiu este capabil să mă identifice sau să-i identifice pe prietenii mei, precum și să înregistreze tot ceea ce facem. Chiar și mai mult mă îngrijorează o întrebare: dacă poate fi amplasat echipament în spațiu care să ne monitorizeze fiecare mișcare cotidiană, fără ca noi să putem spune ceva în această privință, ce altceva pot ei lansa pe orbită, deasupra capetelor noastre, și ce va face acel lucru? Progresul științific adus de cursa pentru cucerirea spațiului și de inițiativa „Războiul Stelelor” a lui Ronald Reagan a scăpat de sub control, iar acum în Statele Unite se vorbește despre războaie purtate în spațiu.

Cel mai puternic mijloc de a-și spiona inamicii și cetățenii de care dispune America este satelitul „Keyhole” (KH – „gaura cheii”). Fiecare costă 1 miliard de dolari și, totuși, tot ceea ce se știe deocamdată despre mișcările sale în spațiu este că operează la diferite altitudini de alți sateliți – detaliile orbitelor lor de deasupra Pământului sunt strict secrete.



Numărul exact de sateliți KH activi este de asemenea necunoscut, deși în general se acceptă că există vreo 200 pe orbite „fixe” (adică se mișcă cu aceeași viteză ca și Terra, așa că rămân în aceeași poziție în raport cu planeta de sub ei) și că grămezi dense sunt poziționate deasupra unor locuri cu probleme, precum Orientul Mijlociu și Coreea de Nord.

Sateliții artificiali sunt creați pentru a îndeplini funcții specifice. Un satelit de comunicații, de pildă, îmbracă de obicei forma unei farfurii sau umbrelor, cu antene multiple. Flota KH este cheia succesului lui Echelon, cel mai mare sistem colector de informații din toate timpurile, și, de asemenea, a dezvoltării și a utilizării de arme în spațiu. Sateliții KH sunt lansați pe orbită de pe navete spațiale NASA sau de pe rachete Titan. În esență, ei sunt camere digitale orbitale, echipate cu lentile foarte puternice, capabile să detecteze obiecte de pe sol care nu au mai mult de 12 centimetri de-a curmezișul. Asta înseamnă că pot citi plăcuțe de înmatriculare ale autovehiculelor sau titlurile dintr-un ziar, precum pot și să identifice o bandă de încărcare a unei arme. Programul camerei de supraveghere scanează obiectul și fie îl înregistrează imediat, fie, dacă vizibilitatea este proastă, ia o decizie automată de a produce o imagine de calitate mai bună. Imaginile transmise de sateliți sunt analizate la Agenția Națională de Imagistică și Cartografiere, care oferă agențiilor de securitate guvernamentale, la cerere, datele obținute.

În teorie, informațiile adunate de sateliții KH pot fi folosite pentru colectarea de date din spionajul militar sau pentru cercetarea științifică. Totuși, NSA și CIA beneficiază și ele de aceste informații, deoarece se știe, din dovezile aduse în tribunalele americane, că polițiile au folosit sateliții pentru a-i spiona pe cetățenii americani considerați „potențiali teroriști, persoane care pot încălca legea sau crea probleme”. Altfel spus, practic oricine poate fi vizat ca subiect al observației de flota sateliților ce orbitează Pământul.

Cunoștințele științifice necesare pentru a trimite senzori și pentru a lansa echipamente de filmare sofisticate pe o orbită stabilă deasupra planetei s-au dezvoltat rapid din primele zile

ale cuceririi spațiului, iar sistemele de „ridicare” care plasează sateliții în spațiu operează acum din întreaga lume. Unele mașinării spațiale sunt capabile să îndeplinească misiuni sofisticate și, ocazional, agresive. Este poate de înțeles faptul că atât de mult efort și resurse sunt utilizate în știința tehnologiei sateliților, având în vedere impactul pe care primul satelit artificial, Sputnikul sovietic din 1957, l-a avut asupra moralului națiunii americane când a fost lansat. Pe atunci, el a provocat mare îngrijorare, vecină cu panica, în Statele Unite. Chiar dacă Sputnik nu făcea în mare decât să transmită „bipuri” printr-un radio ieftin ce plutea deasupra capetelor lor, americanii au simțit că spațiul lor aerian era violat, ceea ce i-a făcut să se simtă foarte vulnerabili. Tehnologia este astăzi mult mai rafinată. De la înălțimi de peste opt kilometri, satelitul de spionaj modern poate urmări și înregistra toate activitățile noastre cotidiene. El are senzori de căldură și tehnologii de obținere a unor imagini cu rezoluție mai bună, care îi permit să ne supravegheze în continuare, oriunde ne-am afla. Nu contează dacă o țintă umană se plimbă pe stradă sau conduce cu viteză pe autostradă sau se află în interior (într-o pivniță sau în ungherele ascunse ale unei fortărețe). Nici vremea nu schimbă cu ceva lucrurile. Subiectul poate la fel de bine să stea într-o închisoare sau în mijlocul unei furtuni cu trăsnete.

Deși pe orbită se află numeroși sateliți-spion, de fapt nu e nevoie decât de trei astfel de sateliți de ultimă generație pentru a „vedea” întreaga lume. Pe lângă faptul că au puterea de a captura și retransmite către sol imagini în timp real, ce altceva mai pot face ei? Pot controla de pe orbită sisteme de supraveghere electronică terestre sau să ne intercepteze conversațiile din spațiu sau chiar să lanseze arme? Americanii s-au bazat foarte mult pe tehnologia sateliților în timpul războaielor purtate de ei în Afghanistan și Irak. Această tehnologie le-a permis să intercepteze cantități vaste de informații din comunicații, prin sistemul Echelon, și să le retransmită către sediul CIA din Langley, Virginia, prin Sediul Comunicațiilor Guvernamentale (GCHQ), Menwith Hill și

multe alte stații.

Desigur, americanii nu sunt singura națiune ai cărei sateliți de supraveghere orbitează Pământul. Spațiul forfotește de aparaturi ocupate să înregistreze și să transmită sau care doar dau ocol planetei, precum niște corăbii aeriene. În prezent există 3.000 de sateliți artificiali care operează pe orbită deasupra Pământului. Flota de sateliți Astra, care transmite programe pentru B SKYB, are 12 sateliți care orbitează la 35 880 de kilometri de Terra. Din cei 200 de sateliți „Keyhole” americani lansați de la începutul anilor 1990, se crede că în jur de 150 funcționează încă. Restul de 50 sunt excedentari și s-au alăturat celor 6.000 de bucăți de deșeuri spațiale care orbitează planeta.

Grație disponibilității largi de imagini de rezoluție mare prin satelit, provenind din surse civile nerestricționate, chiar și națiunile mai puțin prospere pot obține acces instantaneu la supravegherea prin satelit, dacă își permit să plătească pentru ea. Imagini de valoare militară evidentă pot fi achiziționate acum de efectiv orice țară. De fapt, deși puține națiuni își permit să conducă propriile programe de spionaj prin satelit, IKONOS, Quickbird și alte sisteme private sunt accesibile în fond oricărei țări, iar calitatea serviciilor oferite de ele este la un standard suficient de ridicat pentru a fi folosite chiar de CIA și NSA.

Echipamentele de spionaj și militare furnizează cele mai multe date „SIGINT” (semnale de spionaj) și fotografice devorate de agențiile de spionaj și de forțele de poliție din Marea Britanie și America. Dacă vezi imaginile pe care ele sunt capabile să le transmită înapoi, îți va fi aproape imposibil să accepți distanța de la care au fost luate. Departamentul guvernului american cel mai implicat în tehnologia de supraveghere prin satelit este Agenția pentru Proiecte de Cercetare Avansată (ARPA), un braț al Pentagonului. NASA se ocupă de sateliții civili, dar nu există o linie strictă ce separă funcțiile civile și militare. Administrația Națională pentru Aeronautică și Spațiu (NASA) lansează toți sateliții americani fie din Cape Kennedy (Florida), fie din baza forțelor aeriene

Vandenberg (California) – indiferent dacă ei sunt operați de Armată, CIA, corporații sau lansați experimental de NASA ori pentru cercetarea spațiului. E dificil de făcut o distincție rapidă între sateliții guvernamentali și cei privați; cercetările realizate de NASA sunt deseori aplicabile tuturor tipurilor de echipamente de pe orbită. Nici ARPA, nici NASA nu se ocupă cu producția de sateliți; în schimb, ele garantează tehnologia, în timp ce diverse corporații furnizează echipamentele.

Armata americană își limitează deocamdată activitatea prin satelit la supraveghere, navigație și comunicații. Dar pare sigur că forțele militare își vor extinde capacitățile până la a avea în viitor armament în spațiu. Unul dintre motivele declarate pentru asta e faptul că există deja comerț activ în spațiu (sub forma sateliților de comunicații) și acesta va avea nevoie să fie protejat. Oriunde ajunge comerțul american, acolo există și interesul național și necesitatea apărării lui. În 2002, Paul Teets, subsecretarul Forțelor Aeriene și directorul Biroului Național de Recunoaștere, a declarat într-un discurs public că, în opinia sa, armele vor ajunge în spațiu, iar asta „e doar o chestiune de timp”. Teets știe probabil ce zice, cu experiența sa în dezvoltarea armelor de precizie, precum rachete și bombe cu acuratețe de 1 metru. Bombele ghidate prin laser și rachetele ghidate prin GPS; precum Tomahawk, le-au dat deja forțelor militare o putere imensă, care poate garanta înfrângerea oricărui inamic cunoscut într-un război convențional și care, cu o tehnologie a sateliților corect desfășurată, poate – cel puțin teoretic – să elimine victimele colaterale (civile). Trendul se îndreaptă către sisteme de armament mai precise și letale, deseori controlate de la distanță, capabile să răspundă comenzilor în câteva secunde și să atace obiective de oriunde în lume, care au fost identificate de sateliții „Keyhole”. Pornind de aici, tehnologia spațială și utilizarea ghidării prin satelit vor oferi avantaje semnificative în viitoarele ostilități. Guvernul Statelor Unite, după experiența sa de succes cu tehnologia spațială în războiul purtat în Irak, studiază în mod activ următoarea generație de armament – armele laser și „cinetice”. (O să examinăm în

curând ce pot face acestea.)

Potrivit ziarului *Washington Post*, președintele Statelor Unite și comandanții săi militari au acceptat că un anumit conflict în spațiu este acum inevitabil și se pregătesc pentru el. Abordarea reținută a sistemelor de tip „Războiul Stelelor” din partea administrației Clinton a fost înlocuită de acceptarea fără rezerve de către administrația Bush a exploatării inevitabile a spațiului în scop militar. Este o perspectivă alarmantă. Tehnicienii nu doar studiază modalități prin care putem fi protejați din spațiu, ci plănuiesc, de asemenea, folosirea tehnologiei spațiale pentru a ne ucide.

Totuși, costurile rămân marea problemă. „Ridicarea” sateliților este costisitoare în SUA. De aceea, furnizorii de sateliți comerciali utilizează unitățile de lansare din țări precum China, unde costurile sunt mai mici. Unul dintre cele mai importante astfel de locuri din afara Statelor Unite este Baikonur, din Kazahstan. Pentru a opera în mod tactic sateliții, astfel încât ei să poată fi ridicați pe orbite mai depărtate, e nevoie de cantități enorme de energie. Noile generații de sisteme de înaltă putere sunt de asemenea necesare pentru a activa și întreține arme ce folosesc lasere cu înaltă energie, evitând astfel reîncărcări frecvente și costisitoare. S-a manifestat mult interes pentru tehnologii ce pot ajuta la micșorarea viitoarelor platforme spațiale și la reducerea cantității de energie necesară pentru lansare. Dispozitive mici, numite microsisteme electromecanice (MEMS), vor detecta căldura, lumina, mișcarea și sunetul; ele pot fi utilizate într-o varietate de aplicații spațiale, printre altele supravegherea și controlul suprafețelor reflectorizante din sisteme laser spațiale.

Fiecare sistem de armament dezvoltat și lansat va presupune un întreg „sistem de sisteme”, pentru a integra funcțiile de supraveghere, colectare, detectare și evaluare a daunelor de război. Statele Unite prevăd pleiade de sateliți, care vor fi mai puțin vulnerabili în fața atacurilor, în timp ce acum, dacă un singur satelit ar fi atacat, asta ar putea scoate din circulație întreg sistemul. Câteva grupuri de sateliți,

gravitând la distanțe mici, ar putea oferi o acoperire globală „24 de ore pe zi, șapte zile pe săptămână”. Asta înseamnă că populația lumii ar putea fi sub o amenințare constantă din partea unor arme aflate pe orbită, conectate cu sisteme de supraveghere.

Armele laser sunt pe cale să devină parte a arsenalului unei superputeri. Au fost deja concepute și construite lasere chimice cu oxigen și iodină, care pot fi utilizate și ca arme. Laserele chimice sunt cercetate de când administrația Reagan a propus sistemul de apărare împotriva rachetelor „Războiul Stelelor”, în anii 1980. În ultimii 20 de ani, aceste arme au cunoscut ameliorări semnificative în ceea ce privește sistemul optic, miniaturizarea, generarea de energie, controlul automat și identificarea țintei prin intermediul sateliților de supraveghere. Există tehnologia necesară pentru a produce un prototip care va permite atacarea țintelor în câteva secunde sau minute – oriunde în lume. Forțele Aeriene Americane vor lansa acest tip de laser în sistemul lor ABL (Airborne Laser Sistem – Sistem Laser Aerian). Creat pentru apărarea de rachete balistice, el va fi în curând utilizat în mod regulat. Dezavantajele sistemului ABL sunt că trebuie aeropurtat pentru a fi eficient în timpul unui atac cu rachete balistice. Acest lucru face ca un sistem de arme laser aflate în spațiu – și în permanentă stare de așteptare – să fie alegerea preferată de forțele armate. Un sistem de arme laser din spațiu ar oferi o acoperire constantă, dacă ar fi utilizată o cantitate suficientă. Totuși, armele laser nu sunt dintre cele care pot fi folosite pe orice vreme. Norii, ploaia și efectele atmosferice pot disipa razele laser, impunând, astfel, creșterea puterii utilizate, pentru a le compensa. Totuși, ele simt arme flexibile, prin aceea că se poate controla cantitatea pagubelor produse, cu ajutorul duratei pulsului și al puterii radiației; Materialele inflamabile vor lua foc la niveluri de irradiație destul de reduse, făcând mai ales din rafinăriile de petrol niște ținte vulnerabile. La niveluri de putere superioare și cu o durată mai mare (care poate ajunge la câteva secunde), laserul poate să ardă și să distrugă și o țintă mai solidă. Laserele de mare

putere s-au dovedit eficiente deja în doborârea de rachete balistice, aflate în etapa de ascensiune, când sunt pline de combustibilul necesar învingerii gravitației Pământului. De îndată ce se vor dezvolta în mod corespunzător și generațiile de lasere de mare putere, iar tehnicile de miniaturizare vor fi folosite pentru a se rezolva ridicarea instrumentelor pe orbită, armele laser spațiale vor fi gata de a fi produse și utilizate.

Americanii mai dezvoltă însă și un al doilea sistem de arme spațiale, care folosește tehnologia numită „cINETICĂ”. Armele cinetice sunt proiectile lansate de pe platforme din spațiu și ghidate prin GPS sau prin laser designator, o sursă de lumină laser utilizată pentru luminarea țintei. Armele cinetice sunt extrem de precise, deoarece ele folosesc sisteme de ghidare similare cu cele utilizate de bombele și rachetele cu ghidare de precizie – însă fără explozibili. Rachetele își obțin marele potențial distructiv prin viteza pe care o ating. Ajungând la o viteză hipersonică, ele pot produce forțe enorme, capabile să facă praf practic orice țintă. Se spune că o armă cinetică poate distruge buncăre de comandă sau pline cu muniție, aflate la sute de metri sub pământ, în funcție de tipul de proiectile folosit, pot fi atacate ținte singulare sau multiple.

Spre deosebire de lasere, armele cinetice vor putea fi folosite în orice condiții atmosferice, putând fi lansate din sateliți și să lovească ținte aflate oriunde pe pământ, în numai câteva minute. Aceasta le dă un avantaj imens față de lasere. Un alt avantaj este acela că armele cinetice nu necesită cantitățile imense de energie de care au nevoie armele laser. Ele vor opera în tandem cu sateliții de supraveghere și de țintire „Keyhole” și vor fi lansate dintr-un grup de arme-sateliți, lucru care le face, astfel, foarte dificil de atacat. Principala problemă a armelor cinetice o reprezintă căldura pe care o generează la reintrarea în atmosfera terestră, care poate deteriora serios receptorul GPS necesar pentru ghidare. Una din posibilele soluții, testată la acest moment, ar implica folosirea unor lasere pentru a crea o undă-scut, care să protejeze proiectilul când trece prin atmosfera terestră: Este imposibil să te mai ferești de o armă cinetică, odată ce aceasta

a fost lansată. Singura măsură defensivă fezabilă împotriva unui atac cinetic ar fi folosirea unor arme antisatelit. Ele ar întrerupe sistemele de navigație prin GPS necesare pentru a ghida armele sau ar elimina satelitul înainte ca acesta să lanseze proiectilul. Tehnologia pentru a produce arme cinetice este deja disponibilă. Orice îmbunătățiri ulterioare pe care le-ar suporta această tehnologie vor fi simple creșteri ale acurateței sau ale potențialului lor distructiv.

Ca factor determinant în influențarea rezultatelor unui conflict și prin aceea că duc la eliminarea totală a nevoii de arme convenționale, ele nu vor altera, totuși, balanța puterii. Este foarte probabil ca, în cele din urmă, armele spațiale să devină un sistem de atac de precizie obișnuit, care mai degrabă sprijină celelalte sisteme de atac, în loc să le înlocuiască.

Războaiele conduse din spațiu le vor permite comandanților – care, bineînțeles, se vor afla departe de câmpul de bătălie – să folosească sisteme de sateliți fără echipaj, pentru a realiza supravegherea, identificarea țintei și distrugerea ei. Armele spațiale vor avea cu adevărat o arie de cuprindere globală. Prima parte a programului, care este cel mai probabil să ajungă în spațiu, este rețeaua de sateliți de supraveghere necesari pentru identificarea țintelor. Aceștia vor fi mai puternici decât orice a existat înaintea lor, capabili să vadă orice ungher ascuns de pe planetă.

Există motive întemeiate pentru îngrijorarea internațională cu privire la posibilele distrugerii provocate de un război condus din spațiu. Toate țintele strategice vor fi vulnerabile în fața atacurilor. Din pricina reacției rapide și a vitezei armelor laser, tancurile, avioanele, vehiculele blindate, rachetele, elicopterele și navele, aproape orice țintă militară care are o suprafață poate fi ținută și distrusă. Navele aflate pe mare nu vor mai fi imune la atacuri, oriunde s-ar găsi. Acest tip de acoperire globală n-a mai existat până acum. Deși bombardierele fixe B-2 pot acționa cu precizie oriunde în lume, timpul necesar pentru ca ele să-și atingă ținta este mult mai lung decât cel necesar unei arme din spațiu.



Este posibil ca armele spațiale să joace un rol în acțiunile militare pe mare, dar prezența pe timp de pace și misiunile de reacție la criză, incluzând operațiunile amfibii de contingentă, nu vor dispărea niciodată. Marina militară va avea un rol viabil și semnificativ dejucat. Portavioanele, ca piesă de rezistență a diplomației naționale și centru al operațiunilor de reacție rapidă, vor continua să existe. Bineînțeles, ele vor deveni tot mai dificil de apărut și, pe măsură ce tehnologia va evolua, va veni o vreme când nu vor mai avea unde să se ascundă. În cele din urmă, toate națiunile vor trebui să joace un rol în controlarea spațiului, pentru ca fiecare să-și poată apăra dreptul de a folosi spațiul maritim, aerian și terestru. De aceea, orice monopol al Statelor Unite în ceea ce privește desfășurarea de arme ofensive în spațiu ar fi temporar, în cel mai bun caz.

Evident, utilizarea de sisteme de sateliți ofensivi pe timp de pace va crea un imens scandal internațional. Toate națiunile care nu se consideră aliați ai Statelor Unite vor dori să dezvolte sisteme defensive. Supravegherea intruzivă de la bordul flotelor de sateliți „Keyhole” va fi prima țintă. În China, contramăsuri defensive sunt deja în lucru. Aceste măsuri sunt, fără îndoială, mai degrabă limitate pe moment, din cauza costurilor mari de dezvoltare și instalare pe care le presupun, dar este foarte probabil să se îmbunătățească în timp. În ultimul timp, au fost făcute multe încercări de blocare a sateliților de supraveghere americani. Controlul asupra logisticii spațiale, inclusiv logistica antisatelit, va avea în mod clar un impact asupra strategiilor și planificării militare viitoare. Statele Unite au rezistat în decursul istoriei plasării de sisteme de arme antisatelit în operațiuni, de aceea este de așteptat ca sistemele să rămână terestre. Dar, fie că vor avea baza în spațiu, fie că ea va fi terestră, misiunile de control spațial ale Statelor Unite vor trebui extinse. Utilizarea comercială a spațiului este extensivă, în special în domeniul comunicațiilor. Deschiderea spațiului către potențiale conflicte ar fi devastatoare pentru activitățile industriale și comerciale americane. Altfel spus, dacă Occidentului i s-ar

refuza accesul la sateliții de comunicații comerciali, economia americană ar ajunge pe butuci într-un răstimp foarte scurt. Totuși, în general, asemenea viziuni futuriste nu se îndeplinesc așa cum se așteaptă. Armele spațiale pot fi un avantaj formidabil pentru comandații viitorului, însă un general va continua să se bazeze pe resursele convenționale. La fel cum armele nucleare nu au înlăturat cerința de capacități convenționale robuste, care includ flote și armate, este evident că armele ofensive cu baza în spațiu nu vor satisface toate nevoile militare – și oricum, după cum am mai discutat, împotriva lor se dezvoltă deja contramăsuri.

Tehnologia informației și cantitatea imensă de date pe care, în acest moment, comandanții din teren se bazează atât de mult, vin acum predominant cu ajutorul sateliților de comunicații. Chiar și așa, câteodată sunt insuficiente. Statele Unite investesc masiv în sisteme de rezervă, prin folosirea Vehiculelor Aeriene fără Echipaj (UAV-uri), care simt capabile să ofere în timp real supraveghere, informații secrete și informații despre ținte. Sarcina lor este să devină o alternativă la sateliți sau la acum demodatele avioane teleghidate „Predator”, care s-au dovedit atât de valoroase pentru supravegherea avansată în Războiul din Irak. Companiile britanice furnizează sisteme video și GPS care sunt utilizate de oamenii de știință americani ce dezvoltă roboți de supraveghere. University College din Londra a dezvoltat un vehicul de recunoaștere sub forma unui șarpe, conceput a se mișca pe pământ în maniera reptilei pe care o imită. El va fi lăsat la pământ dintr-un avion teleghidat și va purta asupra sa instrumente capabile să transmită detaliile pozițiilor inamice. Computerul său se poate adapta, astfel încât să continue să transmită chiar și după ce ar fi distrus. UAV-urile au fost dezvoltate pentru misiuni de recunoaștere în clădiri, tuneluri și peșteri. Alimentate de ventilatoare contrarotante și echipate cu aparatură sensibilă vizual, acustic și în infraroșu, ele plutesc deasupra câmpurilor de luptă urbane și transmit înapoi către liniile americane informații secrete.

O largă varietate de UAV-uri de toate tipurile (cum ar fi

„Predator”) reprezintă acum o priveliște familiară deasupra Irakului. Ele sunt ieftine, discrete și tind să fie folosite în special pentru adunarea de informații și pentru supraveghere. Însă există o tendință către aparatură de dimensiuni mult mai mici. Încă din 1995 sunt în dezvoltare aparate de zbor microscopice. În ultimii cinci ani, scopul a fost acela de a imita insectele zburătoare, atât în ceea ce privește zborul, cât și mărimea. De exemplu, felul în care un fluture se mișcă în zbor este bine înțeles și poate fi copiat de către oamenii de știință. Au fost construite prototipuri care zboară cu ușurință. Acum 20 de ani, companii americane precum Aeronviroment proiectau și testau mașini de zbor minuscule, alimentate cu baterii pe litiu și care erau încărcate cu echipament de zbor, computer, cameră video și transmițător. Modelele inițiale, precum Văduva Neagră, care funcționa cu ajutorul unei elice, avea 15 cm lungime și cântărea 56g. Era capabil să producă o imagine de mare precizie. Mașinile de zbor miniaturale moderne rămân secrete, deoarece sunt încă folosite, și nu doar de către agențiile secrete, ci și de către companii private, cu scopuri ascunse. În mod clar, un derivat al cercetării militare, aplicat în sectorul privat, va fi abilitatea de utilizare a microroboticii ca mijloc de transport al unor sisteme de supraveghere sofisticate în medii serios protejate.

Acum câțiva ani, Biroul pentru Cercetări Navale al Statelor Unite a construit și testat un prototip de aparat de zbor teleghidat pentru spionaj mai mic decât o monedă de un penny. Variantele recente sunt mai mici, mai puternice și folosesc puterea solară pentru a acționa patru aripi membranare, care se zbat cu 180 de bătăi pe secundă și care le permit să creeze portanță. Aripile poartă pe ele așa-numitul „praf magic” – cipuri microscopice de computer care reprezintă creierul vehiculului, în Statele Unite, au fost raportate insecte zburătoare manufacturate și dezvoltate de Georgia Tech Research Institute – minuscule, telecomandate și produse în masă –, care au fost folosite pentru a se infiltra în clădiri și a rămâne nevăzute. Tehnica este numită „biomimetică”, făcând referință la mimarea sistemelor biologice

și adaptarea lor pentru cerințele umane. „Insectele” pot transmite date la mare distanță. Unele dintre ele sunt folosite în sistemele de ghidare și adaptate la proiectele rapide și ieftine de curățare a minelor. Ele sunt proiectate să profite de condițiile atmosferice proaste pentru a pătrunde cât mai adânc în teritoriile inamice. Au mai fost dezvoltate și alte concepte, care folosesc motoare cu reacție miniaturale, alimentate cu hidrocarburi și capabile să zboare zeci de kilometri cu viteze de 80 km pe oră. RMB Miniature Bearings, o companie elvețiană, a produs motoare electrice care cântăresc o treime de gram. Iar oamenii de știință de la Massachusetts Institute of Technology au dezvoltat un motor cu reacție care măsoară 10 mm pe 3 mm și care este alimentat cu motorină sau benzină.

Bineînțeles, acestea sunt jucării pentru spioni – adevărata muncă murdară este dusă la îndeplinire de către cei care analizează datele culese, de aparatura de spargere a codurilor și de computerele masive încuiate în camere aseptice, în peisaje rurale îndepărtate, peste tot în această lume. Știința roboticii miniaturale și folosirea prafului magic au fost în stadiu de dezvoltare timp de mulți ani, iar Pentagonul n-a dezvăluit stadiul cercetărilor. Nu există nicio îndoială că tehnicile la care au lucrat au produs dividende, atât în colectarea de informații secrete, cât și în supravegherea câmpului de luptă. Problema este că aceste aparate vor trebui operate de către oameni, cărora politicienii le vor spune ce să facă. Și probabil acesta este punctul din care lucrurile ar putea începe să meargă prost.

Tehnologiile militare și cele comerciale se dezvoltă separat, însă sunt reunite regulat pentru aplicații reciproc benefice. Progresul uluitor al tehnologiei civile de supraveghere la distanță aplicată la câmpurile moderne de luptă presupune că tehnologia de luptă a atins deja un stadiu de dezvoltare la limita SF-ului. Impulsul pentru ceea ce a ajuns să fie numită „tehnologia de luptă la distanță” a venit de la americani, care au prevăzut, într-o oarecare măsură, conflictele armate necomplicate de scrupulele morale care bântuie alte națiuni.

Spre deosebire de britanici, care au recurs la acuzarea propriilor soldați care au ucis irakieni în timpul acțiunilor militare împotriva insurgenților, prioritatea americanilor a rămas siguranța forțelor lor armate și a propriilor cetățeni. Chiar și atunci când un soldat american a fost înregistrat pe cameră cum omoară cu sânge rece trei prizonieri răniți și neînarmați, acest lucru nu a dus la acuzarea lui. Statele Unite nu au aderat niciodată la Curtea Penală Internațională, iar dacă un soldat american spune că s-a simțit amenințat atunci când a deschis focul, este foarte puțin probabil ca el să fie acuzat vreodată. De fapt, nu au existat acuzații penale împotriva soldaților americani care au luat parte la bătălie, în timpul sau după Războiul din Irak. Această atitudine le permite să dezvolte tehnologii militare care ar putea să nu fie considerate acceptabile de către forțele armate britanice. Un exemplu ar fi introducerea roboților atât ca instrumente de supraveghere, cât și ca mașini de ucis.

Utilizarea de aeronave teleghidate drept vehicule lansatoare de rachete a devenit acum un lucru obișnuit. Programele de dezvoltare a tehnicilor robotice de război – Sistemul Direct de Acțiune pentru Observarea și Recunoașterea Armelor Speciale (SWORDS) – și armele pe care le-au dezvoltat au fost utilizate în situații de luptă din Afghanistan și Irak. La începutul anului 2005, America a început să trimită roboți înarmați în Irak. Roboții aveau inițial un rol de recunoaștere în teritoriul inamic, dar și capacitatea de a executa foc mortal. Acești roboți ai începuturilor sunt de fapt vehicule monitorizate, telecomandate, care pot fi operate de la o distanță de o mie de metri de către un soldat echipat cu un laptop. Ei sunt înzestrați cu sisteme de navigare prin GPS, camere video și arme automate de foc rapid, iar unele variante pot fi înarmate chiar cu lansatoare de grenade și rachete antitanc.

O mașină poate ucide fără remușcări sau sentimente de vinovăție și poate fi și rapidă. Pentagonul a alocat 70 de miliarde de dolari roboticii militare, într-un program denumit „Sisteme de Luptă ale Viitorului”, iar cu acest gen de investiții

și cu viteza rapidă a dezvoltării tehnologice, în curând roboții vor fi folosiți în mod curent. Totuși, britanicii sunt preocupați de chestiuni etice și de legalitatea acestor roboți pe câmpul de luptă. În august 2004, un pilot al Forțelor Aeriene Regale (RAF), folosind un sistem computerizat, la o bază a Forțelor Aeriene ale SUA din deșertul Nevada, a putut controla un avion teleghidat de tip Predator, care zbura la 3 218 kilometri distanță, deasupra Irakului, și a lansat o rachetă Hellfire direct la țintă – o fortificație a unui grup de insurgenți.

Un fost șef din Comanda Strategică mi-a spus: „Ne antrenăm piloții să evalueze și să identifice țintele înainte de a deschide focul. Pilotul RAF care opera avionul Predator de pe teritoriul Statelor Unite acționa sub incidența legii britanice și a unui regulament de angajare britanic. Dar suntem preocupați de eficiența armelor telecomandate într-un câmp de luptă urban aglomerat. Putem noi să garantăm că un robot va putea să facă distincția între un insurgent armat și o femeie cu un copil mic în brațe? Cum poți să programezi un robot să ia decizii de viață și de moarte cu viteza fulgerului, în condiții haotice de luptă? Un soldat trebuie să se bazeze pe instinct și antrenament și trebuie să ia decizii dificile instantaneu. Nu cred că ne putem aștepta încă la așa ceva din partea unei mașini. Am fi îngrijorați de posibilitatea ca mașina să funcționeze prost. Știința roboticii de luptă se află încă la începuturi și se bazează pe tehnologii precum semnalele radio și transmiterea de imagine, lucruri cu care se poate ușor interfera”.

Schimbări revoluționare în modul în care sunt conduse războaiele și supravegherea în secolul următor nu pot fi prezise bazându-ne doar pe prezența armelor spațiale ofensive, a roboticii și a dezvoltării sistemelor de supraveghere miniaturale. În cele din urmă, războiul se reduce întotdeauna la un conflict uman – om contra om, esența bătăliei. Scopul ultim al cercetării în domeniul roboticii este acela de a produce o mașină care să poată face tot ce poate face un soldat. Americanii estimează costul eventual al unui astfel de robot la aproximativ 10% din cel al contrapartidei

sale umane. După Geoff Grossman de la Centrul de Cercetări al Forțelor Unite Americane, deocamdată, tehnologia poate oferi puterea de procesare computerizată echivalentă celei a unui mamifer.

Armele antisatelit vor avea un loc semnificativ în planificarea militară viitoare, care folosește tehnologia din bazele terestre sau spațiale. Nicio țară nu a admis efectiv că plănuiește sisteme de arme antisatelit, și în niciun caz în spațiu. Dar dezvoltarea armelor laser și a celor cinetice merge înainte și ar putea în curând să însemne folosirea de arme în spațiu, lucru care ar duce la încă o cursă a înarmării. Nu există răspunsuri ușoare. Pe moment, Statele Unite și Marea Britanie, cu tehnologia Echelon filtrată prin flota proprie de sateliți Keyhole, au obținut cea mai mare realizare a spionajului pe care a cunoscut-o vreodată lumea. Iar acum se discută despre cum vor fi înarmate sistemele de supraveghere.

Există multe întrebări la care politicienii și strategii militari americani trebuie să răspundă. De exemplu, vor putea Statele Unite să-și permită noi sisteme de arme spațiale? Se vor abține celelalte națiuni de la a contrabalansa eforturile americane în spațiu, odată ce Statele Unite vor încălca moratoriul privind armele în spațiu? Iar aceste arme spațiale ofensive vor amenința oare stabilitatea lumii? Mulți vor argumenta că e timpul să se cadă de acord asupra interzicerii oricăror arme în spațiu. Tehnologia sateliților și tehnica de război bazată pe aceștia necesită un nou set de reguli de conduită de război și dezvoltarea de noi strategii de către armate.

Instalarea de arme spațiale ofensive pe orbită va fi o chestiune controversată, și nu doar în Statele Unite, ci oriunde în lume. Politicienii și oamenii de știință vor dezbate problema înainte ca „Ultima Frontieră” să devină un câmp de luptă. Este probabil ca publicul american să susțină armele spațiale defensive, cum ar fi sistemele antisatelit, în special ca urmare a lui 9/11. Într-adevăr, mulți americani par să creadă, având în vedere ce consideră ei a fi amenințarea „terorii globale”, că dorința de intimitate este o chestiune futilă, că folosirea unor tehnologii de supraveghere prin satelit mai

intruzive și desfășurarea de arme spațiale sunt de la sine înțelese. Statele Unite ar putea deveni atunci prima națiune care să încalce moratoriul internațional cu privire la plasarea de arme ofensive în afara atmosferei Pământului. Înmarmarea unilaterală a spațiului ar reprezenta un dezastru pentru relațiile dintre Statele Unite și aliații lor de oriunde de pe glob. Deși nu vor fi încălcate niște tratate anume, orice urmă de încredere că Statele Unite ar fi dispuse să respecte aceleași reguli de conduită internațională ca și alte țări ar dispărea pentru totdeauna. Marea temere a majorității țărilor este aceea că, dacă militarizarea spațiului ar începe din cauza unui electorat american dezinteresat, consecințele potențiale vor fi devastatoare – ar putea însemna distrugerea planetei. Ar fi corect să spunem, totuși, că administrația Bush nu a părut prea preocupată. Pare de neconceput că armele spațiale ar putea vreodată să atingă puterea distructivă a celor nucleare. Desfășurarea de arme nucleare în spațiu ar marca, în mod potențial, începutul sfârșitului rasei umane. Dar, deoarece „războiul spațial” se află încă în primele sale faze, armele nucleare ar putea fi privite pur și simplu ca instrumente de descurajare. Fără îndoială că politicienii vor invoca scuza că armele nucleare din spațiu nu vor fi folosite decât în circumstanțe excepționale. Însă cine va decide care sunt aceste circumstanțe?



## Capitolul VIII

### Lege și dezordine

*Forțele de poliție britanice se confruntă cu o nouă lege penală la fiecare trei zile. Este, desigur, foarte greu să ții pasul cu o asemenea irosire a resurselor, provocată de birocrăție, coduri de conduită, cazuri-test și o mulțime de alte accesorii care însoțesc de obicei noua legislație.*

*De la 9/11 încoace, atât în Marea Britanie, cât și în Statele Unite s-au emis un număr enorm de noi legi. Marea Britanie a adoptat Legea de prevenire a actelor teroriste, iar Statele Unite – Actul Patriotic. Ambele seturi de legi au apărut odată cu dovezi vădite de intensificare a măsurilor de securitate, ceea ce include și o supraveghere mai accentuată a populației. Obligate să se confrunte cu fanatici care, ni se spune,ucid fără milă și la întâmplare, ambele guverne au declarat că trebuie să adopte legi mult mai dure, pentru a se asigura că ucigașii sunt luați de pe străzi și ținuți departe de societate.*

Această legislație este, în orice caz, foarte controversată. Cum adesea nu există suficiente dovezi pentru a garanta condamnarea unor suspecți de terorism, noile legi permit statului să închidă cetățenii fără a le asigura un proces corect. De aceea, ele sunt privite ca fiind neliberale și împotriva vechilor tradiții americane și britanice. Inerente acestor legi sunt răspândirea colectării și a stocării informațiilor personale și a spionării cetățenilor.

În Marea Britanie, Legea protecției datelor și Legea libertății informației au fost adoptate pentru a ne proteja și, cel puțin la nivel teoretic, pentru a ne asigura dreptul de a ști precis ce informații cu privire la noi înșine sunt deținute de alte persoane. Cât de protejați ne fac să ne simțim toate

acestea?

Administrația Bush, a susținut întruna că „transformăm salvarea vieții americanilor într-o prioritate” și a încercat să transforme Statele Unite într-o fortăreață, aruncând la gunoi, în timpul procesului, cartea drepturilor cetățenești. Brutalitatea împotriva deținuților arabi de la Abu Ghraib și nu numai reprezintă o politică deliberată. Secretarul apărării Donald Rumsfeld a subliniat foarte clar că Armata Statelor Unite va întreprinde orice este necesar pentru a obține informații de la orice persoană despre care se crede că ar putea deține informații privind un eventual atac asupra Statelor Unite. Umilirea sexuală a arabilor este o metodă eficientă de constrângere. Societatea arabă consideră adesea că victima unei torturi de natură sexuală este singura răspunzătoare pentru soarta ei. Astfel, revelarea abuzului în fața comunității din care face parte victima este mai dăunătoare decât abuzul în sine. Bărbații și femeile răspunzători pentru abuz ori au respectat niște ordine, ori au dezvăluit latura întunecată și violentă a sufletului american.

De curând, în timp ce hoinăream pe străzile din Manhattan, m-am oprit într-o cafenea Starbucks și am luat un exemplar din *New York Times*. Am citit că CIA a recunoscut că a torturat prizonieri în Irak și în alte părți ale globului, precum și că Ministerul Justiției a cercetat un număr de cazuri în care deținuții au murit în timpul detenției ca urmare a interogatoriilor Agenției. P.J. Gross, directorul CIA, a declarat în fața Congresului, în martie 2005, că toate interogatoriile se făceau în condiții legale „în momentul actual”. Când i s-a cerut, sub presiune, să facă aceeași declarație categorică în ceea ce privește tehnicile de interogare pe toată perioada scursă de la 11 septembrie 2001, el a refuzat să dea curs cererii. O expertiză juridică emisă de Ministerul Justiției în 2002 respecta o definiție restrânsă a torturii. Acest fapt permitea Agenției să recurgă la o gamă largă de practici coercitive împotriva persoanelor suspectate de terorism, încarcerate în locuri ținute secrete pe tot cuprinsul globului, fără a fi vinovată de „tortură”. În orice caz, CIA a utilizat

metode de interogare considerabil mai brutale decât cele ale altor agenții militare sau civile. Iar folosirea tehnicii „transferului” de către CIA, ceea ce presupune predarea deținuților autorităților din țări ca Egipt sau Siria, recunoscute pentru utilizarea unei game largi de tehnici de constrângere mentale și fizice, a fost acoperită de către presă. CIA pare că privește trimiterea suspectilor către țări din lumea a treia, spre a fi brutalizați, drept un mijloc de a rămâne cu mâinile curate.

Actul Patriotic” din Statele Unite a intrat în vigoare în timpul perioadei de haos imediat următoare evenimentelor de la 11 septembrie. El a trecut de Congres în grabă, fără o dezbatere adecvată, la doar trei săptămâni de la tragedie. A fost semnat de președintele Bush pe 26 octombrie 2001, fără niciun raport al Camerei sau al Senatului. Este, oricum l-ai privi, un act legislativ draconic, în care expresia „act patriotic” este exprimarea specifică relațiilor publice preferată, Actului de unificare și întărire a Statelor Unite prin furnizarea de mijloace care să intercepteze și să împiedice actele teroriste”. Legea este o versiune de compromis a Actului antiterorism din 2001 și a introdus zeci de schimbări constituționale pentru a crește puterile operaționale ale agențiilor de spionaj și de impunere a legii. Ea conține prevederi care extind drepturile statului de a monitoriza și intercepta schimburi de informații private și chiar dă FBI-ului acces la înregistrările vânzărilor de cărți sau la datele bibliotecilor privind împrumuturile, din care specialiștii își pot forma păreri cu privire la convingerile politice ale cetățenilor.

Actul Patriotic” permite guvernului Statelor Unite să intercepteze informații transmise prin internet sau să limiteze libertățile cetățenilor cu ajutorul noilor tehnologii. El permite, de asemenea, agențiilor specializate folosirea tehnologiilor de comunicare ultramoderne, fără a raporta Congresului, iar această stare de fapt are grave implicații pentru cetățeni ai unor țări din afara Statelor Unite, în principal Canada și Marea Britanie. Actul conține multe prevederi privind supravegherea electronică, prevederi care fuseseră propuse

înainte de distrugerea turnurilor gemene și care au fost, la vremea respectivă, subiectul unor dezbateri și critici aprinse. Una dintre consecințele evenimentelor de la 11 septembrie este imediata reducere la tăcere a oricărei opoziții semnificative provocate de implicațiile asupra libertăților cetățenești pe care le-ar putea avea măsurile antiterorism. Administrația Bush a tensionat și mai mult atmosfera, precizând că are informații conform cărora alte atacuri asemănătoare sunt iminente și că, fără, „Actul Patriotic”, guvernul ar fi paralizat și incapabil să riposteze. Procurorul General John Ashcroft le-a acordat membrilor Congresului doar o săptămână pentru a dezbate și a adopta legea, precizând că, dacă nu o fac, vor purta răspunderea pentru viitoarele atrocități comise de teroriști. John Podesta, șeful personalului de la Casa Albă între 1998 și 2001, a remarcat că atitudinea Congresului s-a transformat, peste noapte, din precauție extremă în consimțirea de a permite forțelor de impunere a legii „reîntoarcerea la o eră în care ele puteau monitoriza și hărțui civili care pur și simplu își exercitau drepturile stipulate în Primul Amendament”.

Un singur senator, Russ Feingold, s-a opus Actului în perioada de haos de după 9/11. El s-a declarat convins că acordarea de puteri crescute agențiilor în ceea ce privește supravegherea electronică nu va duce la o exercitare adecvată a acestora. „Dacă proiectul de lege îi acordă Procurorului General puteri sporite în ceea ce privește relația cu imigranții, cine credeți că vor fi cei care vor suporta abuzurile provocate de aceste puteri? Nu imigranții din Irlanda, El Salvador sau Nicaragua, nici măcar cei din Haiti sau Africa. Vor fi cei din țările arabe, musulmane sau din sudul Asiei. Guvernul nostru a primit noi puteri imense și efectul lor va cădea cel mai puternic pe umerii unei minorități a populației noastre, cei care simt deja foarte acut consecințele acestui dezastru de la 11 septembrie”.

Ar fi incorect să las impresia că monitorizarea comunicațiilor electronice din întreaga lume a fost privită de către Statele Unite drept o responsabilitate doar a lor.

Guvernul Statelor Unite a făcut presiuni asupra tuturor democrațiilor pentru ca acestea să-și perfecționeze legile privind interceptarea comunicațiilor, în așa fel încât tehnologiile noi să fie încurajate. Terorismul reprezintă o problemă globală, prin urmare orice inițiativă împotriva lui trebuie să aibă o dimensiune la fel de globală. Curând după 9/11, fostul director FBI Louis Freeh a primit din partea administrației Bush însărcinarea de a vizita țări în curs de dezvoltare din Europa de Est, Asia și Africă, pentru a promova ideea interceptării comunicațiilor. Statele Unite au susținut, de asemenea, necesitatea garantării ca toate tehnologiile de interceptare să fie prevăzute cu un sistem de supraveghere. Cu alte cuvinte, scopul era să prevină și să facă ilegală fabricarea oricăror echipamente de comunicare sau de supraveghere care, la rândul lor, să nu poată fi spionate și înregistrate.

Majoritatea țărilor democratice își dau foarte bine seama, cu toate acestea, că a trage cu urechea la cetățenii lor reprezintă o politică deloc populară și în niciun caz dezirabilă din partea statului, prin urmare, au inclus în legislațiile și constituțiile lor măsuri de protecție. Marea Britanie, Statele Unite și majoritatea celorlalte democrații sunt obligate prin lege să publice anual numărul interceptărilor comunicaționale autorizate. Aceste țări au regulamente ferme care prevăd ca interceptările să fie autorizate de către un judecător, și asta numai după ce o serie de condiții stricte au fost respectate. Agențiile de spionaj și cele de impunere a legii nu au – cel puțin teoretic – permisiunea de a iniția activități de interceptare înainte de a demonstra că alte metode de investigare au fost încercate, dar s-au dovedit ineficiente. Franța și Marea Britanie au înființat comisii independente pentru a monitoriza abuzurile. Membrii acestor comisii au o înaltă calificare în utilizarea echipamentelor de comunicare și a tehnologiilor de interceptare, precum și puterea de a cerceta toate părțile implicate în supraveghere și – lucrul cel mai important – pentru a pune întrebări incomode. Alte țări, cum ar fi Canada, au numit Comisari ai Vieții Private care au tocmai sarcina de a examina utilizarea corectă sau abuzivă a

supravegherii de către stat.

Unele țări publică anual rapoarte cu privire la utilizarea supravegherii de stat de către diverse departamente guvernamentale. Printre aceste țări se numără Australia, Franța, Canada, Noua Zeelandă, Elveția, Suedia, Statele Unite și Marea Britanie. Însă altele nu sunt la fel de dornice să-și facă publice cifrele. Olanda, de exemplu, și-a relaxat de curând legile privind raportarea interceptărilor de comunicații. La suprafață, faptul că o țară cu o îndelungată tradiție liberală precum Olanda face așa ceva poate părea foarte ciudat. Dar de la asasinarea omului politic liberal Pim Fortuyn și a regizorului radical Theo Van Gogh atitudinea olandezilor cu privire la extremismul islamic din țara lor s-a înăsprit. Faptul că Olanda este țara cu cel mai mare procentaj de imigranți, legali și ilegali, și totodată țara cu cea mai multe interceptări din Uniunea Europeană nu este probabil o coincidență. Pe măsură ce tot mai multe țări intră în UE, permițând tot mai multor non-cetățeni să pătrundă în statele membre – Turcia, prima țară cu adevărat musulmană, abia așteptând să fie admisă –, se înregistrează o atitudine explicabilă de respingere tot mai mare din partea țărilor preponderent creștine, care vor să ridice bariere în calea a ceea ce se tem că ar putea deveni o cucerire culturală și religioasă.

Responsabilitatea instanțelor de monitorizare care controlează supravegherile nu presupune cercetarea doar a interceptării de informații în statele de care țin, ci și a tuturor supravegherilor electronice efectuate la nivel global. Posturile de ascultare ale sediului guvernamental de comunicații din Cheltenham și agenția americană de la Menwith Hill, din Yorkshire, „trag cu urechea” în toată lumea și aproape că nu există democrație care să nu aibă o agenție secretă cu funcții asemănătoare.

Listele publicate ale operațiunilor de supraveghere furnizează informații cu privire la tipul de supraveghere electronică utilizat și precizează și durata pe care acestea au fost active. Justificarea principală pentru asemenea

monitorizări are două capete de afiș: infracțiunile și terorismul. Listele supravegheților sunt publicate pentru a demonstra că activități acceptabile, precum investigațiile jurnalistice, activismul ecologic, drepturile omului, sindicalismul, activitățile religioase și opoziția politică sunt scutite de la supravegherea fără mandat și că aceste grupuri nu reprezintă o țintă doar pentru că ar putea avea conflicte de interese cu cei de la putere. Trebuie, de asemenea, precizat că infracțiunile minore nu pot fi subiectul supravegheții intruzive din motive politice. A face agențiile de siguranță să dea socoteală electoratului monitorizându-le activitățile este un aspect vital într-o adevărată democrație.

Nu trebuie să fii adept al teoriei conspirației pentru a avea încredere în ceea ce privește abuzurile făcute de stat în supravegherea electronică și interceptarea corespondenței. Articolul 17 din Carta Drepturilor Omului cere ca „integritatea și confidențialitatea corespondenței să fie garantate, *de jure* și *de facto*. Corespondența trebuie livrată destinatarului fără a fi interceptată și deschisă sau citită printr-o altă metodă. Supravegherea, indiferent dacă este electronică sau făcută prin alte mijloace, interceptarea de mesaje telefonice, telegrafice sau de alt fel și înregistrarea conversațiilor trebuie interzise”.

Serviciul de Securitate britanic a înregistrat un total de 540 de interceptări în 2004. Cu toate acestea, dezbaterile cu privire la proiectul de lege antiterorism a arătat că interceptările efectuate în scopul de a impune legea au fost constante și larg răspândite în Marea Britanie. Faptul că persoanele suspectate de terorism erau încarcerate fără proces și fără a fi informate de acuzațiile care li se aduc era, potrivit ministrului de interne David Blunkett, justificabil din motive de securitate. Cu alte cuvinte, dacă un suspect ar ști pe baza căror dovezi a fost închis, el și-ar putea da seama de modul în care serviciile de siguranță au obținut informațiile respective. „Interceptările nu pot fi folosite ca dovezi în instanță și eu nu sunt pentru permiterea utilizării lor”, a declarat Blunkett. Adevărul este că majoritatea interceptărilor efectuate de

serviciile de siguranță sunt în afara legii, iar persoanele care le efectuează nu au nici cea mai mică dorință să-și justifice acțiunile în fața unui judecător.

Această reticență lipsește cu desăvârșire în Statele Unite., „Actul Patriotic” este foarte nepopular în multe părți ale Statelor Unite, din cauza modalităților în care eludează prevederile adoptate tocmai pentru preveni folosirea abuzivă a supravegherii cetățenilor de către stat. În februarie 2004, consiliul orașului New York a adoptat o rezoluție ce condamnă încălcarea drepturilor la viața privată garantate de Constituție. Autorii și bibliotecarii au protestat față de secțiunea a cincea a Actului, care permite verificarea înregistrărilor bibliotecilor. Gama de puteri acordate FBI-ului a crescut în mod vizibil din anul în care Actul a intrat în vigoare. Numărul de mandate ce permiteau supravegheri a crescut în 2004, depășind 2000, deci cu mult mai multe decât mandatele federale emise. Acest lucru este cauzat de faptul că, „Actul Patriotic” a făcut supravegherea oamenilor inocenți mult mai simplu de justificat. Și autoritățile canadiene au fost foarte preocupate de această problemă. În noiembrie 2004, comisarul responsabil cu protecția vieții private din British Columbia a prezentat un raport ce sugera că informații personale despre cetățeni canadieni au fost obținute de către autoritățile americane sub protecția Actului, ceea ce violează drepturile canadiene la viața privată. Plângeri referitoare la interceptarea și analizarea schimburilor de informații între cetățeni britanici, ajutate și sprijinite de către compania British Telecom și controlate de către Agenția Națională de Securitate (NSA) la Menwith Hill, s-au lovit de o nepăsare totală.

Implicațiile detaliate ale puterii crescânde a statului au devenit din ce în ce mai evidente pe măsură ce publicul a început să realizeze ce se întâmplă. Există trei legi în cadrul Actului care se referă la interceptarea comunicațiilor de către guvernul Statelor Unite. Titlul III, referitor la interceptarea convorbirilor telefonice și la interceptarea în timp real a comunicațiilor tip voce sau date, stipulează existența unei



„cauze probabile” și aprobarea unui judecător. Este o precauție importantă, care necesită implicarea unei persoane aflate pe o treaptă înaltă a sistemului juridic. Legea privind confidențialitatea comunicațiilor electronice (ECPA) reglementează instalarea de aparate pen-register (care colectează numerele apelate de la un anumit post telefonic) și folosirea unor sisteme de tip „interceptează și urmărește” (care înregistrează numerele ce apelează un anumit post telefonic). Aceste echipamente pot fi folosite pentru a înregistra întreaga activitate pe internet a unei persoane fizice care folosește o linie telefonică. Acest Act nu presupune necesitatea unei „cauze probabile”, iar pentru utilizarea dispozitivelor nu este nevoie decât de un ordin judecătoresc, care poate fi obținut de un avocat guvernamental. Pentru a-l obține, acesta nu trebuie decât să garanteze verbal curții că informațiile sunt relevante în cadrul unei investigații în desfășurare. Astfel, Actul face foarte simplă pentru guvern accesarea informațiilor financiare private, fără a trebui să prezinte dovezi că persoana afectată de acest abuz este suspectată de implicare într-o activitate criminală. O a treia lege, „Legea supravegherii serviciilor secrete străine”, permite utilizarea supravegherii electronice în cazul oricărei persoane care se află în Statele Unite și despre care se crede că ar fi agentul unei puteri străine. Supravegherea necesită numai o „cauză dreaptă” și un ordin judecătoresc, dar îi oferă persoanei fizice o protecție mai puțin consistentă decât în cazul ascultării telefoanelor. Asemenea situații apar când informații cu privire la cetățeni britanici, obținute de americani pe teritoriu britanic, sunt împărtășite cu serviciile secrete britanice.

Diferența dintre Titlul III și Legea privind confidențialitatea comunicațiilor electronice este că primul privește conținutul comunicațiilor, în timp ce ECPA și utilizarea „înregistratoarelor-stilou” și a sistemelor „interceptează și urmărește” privesc, teoretic, doar niște cifre. În consecință, acordul judecătoresc poate fi obținut în urma unei banale declarații a procurorului, iar procedura este foarte indulgentă

cu prevederile ce protejează viața privată din Titlul III. Actul care s-a transformat în lege în octombrie 2001 a redefinit pen-register drept „un dispozitiv sau un proces cu ajutorul căruia se înregistrează sau decodează impulsuri reprezentând sau semnalând informații de la un instrument folosit pentru transmiterea unui conținut informațional de natură electronică” – ceea ce include și e-mailurile trimise de pe un laptop. Un sistem de tipul „interceptează și urmărește” a fost redefinit, în mod similar, ca „un dispozitiv sau un proces care captează impulsuri, electronice sau de altă natură, ce identifică o sursă de informații de la un instrument folosit pentru transmiterea unui conținut informațional de natură electronică”. Aceste „redefiniri” sunt semnificative, pentru că ele permit autorităților să intercepteze și să stocheze imense cantități de informații private, fără acordul unui judecător, pe baza unei simple declarații a unui procuror. Interceptarea poștei electronice, a paginilor accesate cu ajutorul browserelor și a altor forme de comunicare electronică este cunoscută sub numele de „Carnivore” și formează nucleul central al „Actului Patriotic”. Ea este responsabilitatea FBI-ului. Datele pe care Biroul le colectează și analizează sunt, desigur, mult mai consistente decât niște simple numere de telefon, din moment ce pot fi monitorizate site-uri sau alte informații accesate cu ajutorul internetului.

În iulie 2000, Procurorul General al Statelor Unite a creat Consiliul de Supraveghere al Departamentului de Justiție, al cărui rol este examinarea problemelor privind intimitatea și drepturile cetățenești generate de „Carnivore”. În orice caz, când George W. Bush a fost ales președinte, Consiliul a fost înlocuit de un „oficial de nivel înalt”. Raportul nu a fost terminat până la 11 septembrie 2001 și, deloc surprinzător, Congresul nu a putut beneficia de rezultatul cercetărilor atunci când a trebuit să adopte, sub presiune, „Actul Patriotic”.

Pe lângă evidenta natură deloc liberală a Actului, acesta mai are și o alarmantă aură de iresponsabilitate. Pe de-o parte tolerează și încurajează agențiile de impunere a legii care

interceptează comunicațiile și monitorizează cetățenii Statelor Unite, ai Canadei și ai Marii Britanii, și pe de altă parte cedează în fața lobby-ului în favoarea armelor de foc și, cel puțin aparent, pune interesele posesorilor de arme înaintea sfaturilor agențiilor antiteroriste, acestea nemaiputând interveni atunci când suspecții de acte teroriste își cumpără arme. În Statele Unite, grupările fundamentaliste islamice, milițiile radicale și alte grupuri recunoscute ca recurg la mijloace violente pentru a-și promova cauzele au dreptul de a cumpăra arme după bunul lor plac. A-l nega este neconstituțional și o serioasă încălcare a drepturilor lor. Legea precizează că singurele grupuri care nu au voie să cumpere arme sunt criminalii condamnați, imigranții ilegali și persoanele cu tulburări mentale. Asociația Națională pentru Arme de Vânătoare face unul dintre cele mai puternice lobby-uri din Statele Unite și este un apărător fără scrupule ai dreptului de a purta armă. Senatorul democrat din New Jersey, Frank Lautenberg, acuza administrația Bush că apleacă prea mult urechea la lobby-ul armelor de foc, acest interes concretizându-se în anomalii apărute în înregistrările cu privire la posesorii de arme; senatorul cere acțiune imediată. Conform FBI-ului, agenții săi nu au permisiunea de a accesa sau folosi informații despre posesorii de arme și nu au voie să ia măsuri atunci când persoanele suspectate de terorism cumpără arme de foc. Fostul procuror general John Ashcroft nu a permis FBI-ului să compare lista persoanelor suspecte de terorism cu lista celor care au achiziționat arme de foc. „Lista teroriștilor sub supraveghere” a FBI-ului reunește câteva mii de suspecți despre care nimeni nu știe câte arme au achiziționat din 2001 încoace. Nu se știe decât că cel puțin 47 au primit permise de portarmă în cele nouă luni de după iunie 2004. Conform FBI-ului, toate aceste persoane erau teroriști fie dovediți, fie suspecți, și se aflau pe lista monitorizărilor permise de Actul Patriotic”. Astfel, regulile se întorc împotriva FBI-ului, care este obligat prin lege să distrugă orice informații cu privire la posesorii de arme de foc în cel mult 24 de ore de la obținerea acestora.

Legea prevenirii actelor de terorism din Marea Britanie a primit acordul regal pe 11 martie 2005, după un traseu dificil prin Parlament. Legea a introdus un sistem de ordine ale ministrului de interne menite să anihileze activitățile teroriste. Aceste ordine de control permit ministrului să interzică persoanelor suspectate de activități teroriste asocierea cu anumite persoane, folosirea internetului sau a telefoanelor mobile, și să le restricționeze deplasările. Suspecții pot fi urmăriți și supuși arestului la domiciliu. Este o lege dură și neliberală, pentru că se aplică tuturor cetățenilor britanici și anulează prezumția de nevinovăție. Cu toate acestea, există și măsuri de precauție. Ministrul de interne trebuie să apeleze la un judecător de la Curtea Supremă pentru a putea da un ordin de control care nu se abate de la lege, deși, dacă este urgent, poate sări peste acest pas inițial, având obligația de a cere confirmarea Curții în termen de șapte zile. În practică, ministrul de interne poate forța o persoană să rămână în arest la domiciliu, o decizie neconformă cu hotărârile Curții Europene a Drepturilor Omului, dar această decizie trebuie confirmată, după dezbatere, de Parlament în cel mult 40 de zile. Puterile ministrului de interne sunt descrise ca temporare și pot fi pierdute după un an, dacă el nu primește un nou vot de încredere din partea ambelor camere ale Parlamentului. Măsurile de prevedere includ și numirea unui supervisor independent, care trebuie să prezinte un raport Parlamentului, în fiecare an, despre modul în care a fost respectată legea și despre utilizarea ordinelor de control. Proiectul de lege pentru prevenirea terorismului a intrat în vigoare numai pentru că s-a sincronizat cu ceea ce era considerată o criză de securitate fără precedent în Marea Britanie. Întrebarea este cât va dura până când legea va fi abrogată și țara se va întoarce la normal. Mare parte din legile antiterorism intrate în vigoare în trecut au avut tendința să rămână în vigoare ani de zile, dacă nu chiar pe termen nedefinit.

Oricine a încercat să citească Legea protecției datelor din 1998 va observa cât de dificil este să înțelegi exact cum o poți utiliza pentru a-ți proteja propria viață privată. Actul din 1998

este o actualizare a unei legi din 1984 și a intrat în vigoare după dezbateri îndelungate în Parlament. Era deja, lucru cât se poate de previzibil, depășită chiar în momentul intrării în vigoare, din cauza progresului tehnologic foarte rapid. Legea are un comisar al Informațiilor pentru a i se asigura respectarea și permite recursul la Legea drepturilor omului. Acest amănunt nu numai că ajută persoanele fizice, dar joacă și un rol major în modul în care prevederile legii sunt interpretate și puse în aplicare în momentul când un caz ajunge în fața Curții. Există un cod de bune practici ce însoțește legea, iar avocații pot câștiga sume foarte mari reprezentând în instanță persoane care consideră că le-a fost violată intimitatea. La o primă vedere, nu pare să se stipuleze în lege că un șofer ar trebui avertizat dacă mașinii pe care o conduce i se atașează un dispozitiv de urmărire. De asemenea, nu se limitează nici modul în care sunt folosite informațiile obținute de către supraveghetori. Care este poziția legală a unei organizații care strânge imagini cu clienții băncilor în timpul utilizării bancomatelor, dacă aceste imagini sunt furate de o bandă de hoți?

În esență, Legea protecției datelor acoperă orice informație privată care este colectată sau înregistrată, electronic sau pe hârtie. De exemplu, de fiecare dată când furnizezi informații personale unui site, cum ar fi adresa de poștă electronică, adresa poștală, vârsta sau numărul de telefon, site-ul respectiv este obligat, din punct de vedere legal, să te anunțe în ce scop are nevoie de aceste informații și, în același timp, este obligat să-ți dea posibilitatea de a decide dacă poate furniza datele tale unei terțe părți. Ar trebui să-ți ofere o înștiințare privind folosirea informațiilor, ca să precizeze scopul în care este nevoie de datele tale. Când o persoană se abonează la o revistă sau completează un cupon dintr-o reclamă, de obicei ea poate opta să primească informații de la organizații „partenere” în scopuri de marketing (lucruri scrise de obicei cu litere foarte mici). Dacă abonatul refuză, este ilegal ca la datele sale să mai aibă acces altcineva. Organizațiile comerciale pot utiliza datele numai în scopul stipulat în

contract. Site-urile trebuie să precizeze dacă informația furnizată lor va fi codată. Și, dacă o bază de date colectează informații personale, ea este obligată să păstreze informația respectivă pe o durată cât mai scurtă posibil, deși această durată nu este întotdeauna reglementată legal.

Toate neplăcerile provocate de reclamele nedorite pe care le primim pe e-mail pornesc de la cedarea detaliilor noastre personale, în mod ilegal, către o companie de marketing. Legea protecției datelor are scopul de a proteja toate informațiile personale, de la detalii bancare până la înregistrări ale Serviciului Național de Sănătate (NHS), adrese de e-mail sau numere de telefon. Cetățenii unei țări au dreptul de a vedea toate informațiile strânse despre ei de către o organizație publică sau privată. Companiile comerciale trebuie să justifice păstrarea acestor informații. Dacă nu o fac, păstrarea este ilegală, iar informațiile trebuie șterse, conform legii. Datele cerute de cetățeni trebuie furnizate cu cel puțin 40 de zile înainte ca aceștia să poată face reclamație la comisarul Informațiilor.

Legea protecției datelor mai reglementează și ce poate sau nu poate fi făcut în domeniul, aflat în rapidă dezvoltare, al supravegherii. În Marea Britanie, sunt patru tipuri de supraveghere nereglementate prin lege. Mai întâi, este vorba de activitățile de supraveghere intruzive, acoperite de Legea reglementării puterilor de investigare, care se ocupă de antiterorism și infracțiuni grave. Apoi, supravegherea angajaților de către companii care vor să se asigure că personalul se supune contractului semnat la angajare. Al treilea tip este reprezentat de supravegherea cu ajutorul echipamentelor de securitate instalate de proprietari în locuințele lor. În sfârșit, camerele de filmat și echipamentele similare utilizate pentru a transmite imagini în scopuri jurnalistice, artistice sau literare. Legea din 1998 stipulează o serie de standarde de bază. Datele înregistrate prin CCTV trebuie procesate, conform legii, numai în scopuri limitate și în concordanță cu drepturile omului, trebuie să fie adecvate și relevante, să dea dovadă de acuratețe și să nu fie stocate mai

mult decât este necesar. De asemenea, nu este permis ca ele să fie transferate către țări care nu oferă prin lege o protecție adecvată a datelor.

Comisarul Protecției Datelor poate emite preavize de constrângere dacă el sau ea consideră că s-a produs o încălcare a legii. Codul de bune practici intră în posesia oricărei persoane care instalează echipament de supraveghere. El trebuie să fie revăzut în mod regulat, pentru a se lua în considerație schimbările în interpretarea legislației, în tehnologia pentru înregistrarea imaginilor ori a sunetelor, tehnicile de recunoaștere facială și tehnologia digitală, toate acestea fiind tratate în lege.

Când un sistem CCTV este instalat, utilizatorii trebuie să justifice necesitatea acestuia. De exemplu, ei pot fi interesați de prevenirea, investigarea și detectarea unei infracțiuni, de arestarea și punerea sub urmărire a infractorilor, de siguranța personalului și de cea publică sau de monitorizarea securității unei locuințe. Reprezintă o infracțiune instalarea unui sistem ce nu respectă măsurile de siguranță stipulate prin lege. Persoanele implicate în instalarea sistemului trebuie să se legitimeze și să dea o declarație cu privire la importanța utilizării CCTV sau a oricărui alt echipament de supraveghere. Vor trebui să-și justifice opinia și să enumere motivele instalării. Scopurile vor fi aduse la cunoștința Oficiului pentru Protecția Datelor. De asemenea, trebuie precizate persoanele care se vor asigura că funcționarea zilnică a echipamentelor este în conformitate cu codul de bune practici, precum și cu regulile de securitate a documentelor și de confidențialitate. Modul în care imaginile sunt înregistrate trebuie de asemenea să fie în conformitate cu legea, iar echipamentul trebuie instalat într-un loc din care va putea monitoriza numai zona ce se intenționează a fi acoperită. Dacă există spații private în apropierea echipamentelor, utilizatorul va trebui să discute instalarea cu proprietarii spațiilor respective, pentru a obține acordul lor în cazul în care există o cât de mică posibilitate ca echipamentul să înregistreze imagini din acea zonă.

Operatorii sunt obligați să folosească echipamentul numai

pentru scopurile pentru care acesta a fost instalat. Multe sisteme CCTV, cum ar fi cele folosite în centrele oraşelor sau lângă hipermarketuri, sunt adesea foarte sofisticate şi tind să îndrepte camerele de luat vederi spre anumite activităţi, să focalizeze pe anumite persoane, să examineze imagini deja înregistrate pentru agăsi delincvenţi sau martori, sau pentru a observa comportamentul unui angajat. Organizaţiile ce folosesc CCTV pentru orice altceva decât cea mai banală supraveghere trebuie să respecte legea, dar nu toate imaginile lor vor putea fi acoperite în toate circumstanţele. Regula de bază este că posesorii sistemului sunt singurii care decid dacă imaginile înregistrate îi fac să afle o informaţie specifică despre activităţile unei anumite persoane.

În cazul în care camerele sunt reglabile, operatorii nu au voie să le manipuleze pentru a ajunge la zone ce nu au fost precizate dinainte. Dacă restricţionarea zonelor de acces ale camerei, pentru a respecta dreptul la intimitate, este imposibilă, operatorii trebuie învăţaţi să recunoască implicaţiile încălcării vieţii private de către ceea ce filmează. De exemplu, persoanele care fac plajă în grădina din spatele casei se aşteaptă mai mult să aibă intimitate decât cele care tund gazonul în grădina din faţă. Este în regulă ca scopul unui echipament să fie protejarea persoanelor care folosesc un bancomat, dar este ilegal să înregistrezi imagini cu codurile PIN şi situaţia conturilor.

Semne vizibile şi uşor de citit trebuie aşezate în zone uşor accesibile publicului, pentru ca acesta să vadă că zonele respective se află în raza unui echipament de supraveghere. Există reguli clare despre dimensiunea semnelor: ele trebuie să identifice beneficiarul supravegherii, de ce se află echipamentul acolo şi persoana de contact pentru mai multe informaţii. Uneori sistemul de supraveghere poate fi mutat fără avertisment – de exemplu, în cazul în care anunţarea prezenţei camerelor de supraveghere periclitează o investigaţie. În acest caz, sistemul trebuie să fie demontat imediat ce nu mai este necesar.

Există reguli stricte şi în ceea ce priveşte calitatea



imaginilor obținute. Dacă un sistem a fost instalat pentru a detecta sau preveni o infracțiune, imaginile trebuie să fie adecvate, să fie testate cu regularitate și să fie conforme cu normele de calitate specificate în lege. Un „monitor uman” trebuie să se afle la fața locului pentru a decide cum trebuie procedat într-o situație specifică. Declarațiile persoanei respective trebuie înregistrate. Dacă infracțiunea investigată prin această formă de supraveghere are loc noaptea, atunci înregistrarea constantă poate fi realizată doar la momente dinainte specificate, cu camere bine întreținute. Pe durata păstrării imaginilor, integritatea lor trebuie menținută, pentru a asigura valoarea de dovadă și pentru a proteja drepturile persoanelor ale căror imagini au fost înregistrate. Legea precizează că aceste imagini nu trebuie păstrate mai mult decât este necesar. De pildă, dacă nu sunt necesare ca dovezi, imaginile înregistrate în centrul orașelor trebuie șterse după 31 de zile. Vizionarea acestor imagini ar trebui să se facă în locuri restricționate, doar în fața persoanelor care fac parte din personal. Există prevederi stricte cu privire la depozitarea filmelor care ar putea fi folosite ca dovezi la tribunal. Aceste reguli vizează și asigurarea că drepturile indivizilor înregistrați sunt protejate. Orice hotărâre de a face publice imaginile trebuie să respecte legea.

Dacă scopurile sistemului sunt prevenirea și descoperirea infracțiunilor, atunci cedarea imaginilor către terțe părți se poate face numai către agenții de impunere a legii, către reprezentanți legali și mass-media (când este nevoie de ajutorul publicului pentru a identifica victima), către un martor sau un infractor implicat în infracțiune sau către oamenii ale căror imagini au fost înregistrate și depozitate.

Există opt principii pentru protejarea datelor. Acestea sunt precizate în lege și trebuie respectate de orice persoană implicată în supravegherea publicului. Există și un Controlor de Date, care răspunde, în conformitate cu Legea protecției datelor, de inițierea supravegherii. Desigur, Controlorul nu are nicio influență asupra supravegheților inițiate pe ascuns sau asupra interceptărilor de conversații. O privire aruncată pe

site-urile de unde se poate achiziționa echipament de spionaj arată că există o gamă largă de produse pentru cei care vor să tragă cu urechea. O gamă ce se îmbunătățește zi de zi. Și care nu intră sub incidența nici unei legi.

## Capitolul IX

### Rateurile serviciilor secrete

*În ciuda rateurilor agențiilor de spionaj care au făcut posibil atentatul din 11 septembrie, serviciile secrete britanice și americane sunt în continuare incapabile să țină pasul cu evenimentele naționale. O Comisie a Statelor Unite, înființată pentru a monitoriza serviciile secrete, a raportat în aprilie 2005 două lucruri: comunitatea spionilor americani nu numai că s-a înșelat în totalitate în aproape toate concluziile pe care le-a tras înainte de Războiul din Irak, dar este în continuare în ceață în ceea ce privește stadiul actual al programelor nucleare ale statelor ostile – în ciuda faptului că presupusele ambiții nucleare ale lui Saddam au fost unul din principalele motive oferite în favoarea pornirii unui război împotriva Irakului. Agenții precum CIA, FBI, NSA și nou-înființatul Departament al Securității Interne se consideră în continuare mai degrabă rivali decât colaboratori cu aceeași misiune – aceea de a lupta împotriva terorismului mondial. Pentru mulți observatori, un motiv și mai mare de îngrijorare l-a reprezentat manipularea serviciilor secrete în perioada premergătoare invaziei din Irak.*

Nici CIA, nici MI5 nu au reușit să transmită factorilor politici de decizie îndoielile puternice pe care le aveau referitor la una din sursele-cheie de informație asupra presupuselor rezerve de arme de distrugere în masă de care dispunea Irakul.

Poate că a sosit, în sfârșit, vremea când funcționarii publici arată numai ceea ce cred ei că superiorii politici vor să vadă. Cazul teroristului algerian Kamel Bourgass, care a fost închis în 2005 pentru uciderea unui ofițer de poliție și pentru

punerea la cale a unor atentate teroriste, este considerat un exemplu al eșecului serviciilor secrete britanice și al agențiilor de impunere a legii, dar și al altor departamente guvernamentale, inclusiv al serviciului de imigrații. Din când în când, industria de asigurări face publică o estimare a riscurilor teroriste iminente. Amenințările primesc calificative precum: „crescut” (care e rău) și „foarte crescut” (care e și mai rău). De exemplu, Marea Britanie are un risc „crescut” de atac terorist de la începutul Războiului din Irak. Potrivit brokerilor internaționali de asigurări de la Aon, există în prezent opt categorii de teroriști care ar putea amenința Occidentul, iar Marea Britanie este foarte aproape de capul mesei, confruntându-se cu cel puțin patru dintre acestea. Aon ne informează că suntem amenințați de extremiști musulmani, grupări ale militanților pentru drepturile animalelor, grupări teroriste ale republicanilor irlandezi și grupări ale crimei organizate. Și Statele Unite se află sub amenințare, dar lista lor de amenințări include riscuri de atac din partea extremiștilor de dreapta și a extremiștilor religioși. Întrebarea cu care se confruntă publicul este: cât de mare e de fapt amenințarea? Politicienii ne avertizează mereu că o nenorocire e pe cale să se-ntâmple, dar aceasta fie nu se petrece până la urmă, fie este cât pe ce să aibă loc, dar detaliile sunt trecute sub tăcere, pentru ca procesul legal să nu fie pus în pericol. Așadar, ce se întâmplă de fapt? Ce să înțelegem din evenimentele recente?

În ciuda celor mai mari eforturi depuse de guvern, opinia publică britanică a început, inevitabil, să se blazeze în privința amenințării teroriste. Aceasta se poate datora parțial faptului că sistemul judiciar penal britanic se asigură că orice informație care poate periclita un proces corect este ținută departe de domeniul public până la terminarea procesului legal. De la atacul din 11 septembrie, a existat o revărsare de „incidente” teroriste pe teritoriul britanic și, cu toate acestea, publicul a fost ținut departe de ceea ce se petrecea în spatele cortinei. Pe fundalul unei îngrijorări publice generale pentru felul în care Ministerul de Interne se joacă cu drepturile

cetățenești, politicienii continuă să pună placa „pericolului mereu prezent”, avertizând că între Marea Britanie și grupările fundamentaliste există o stare de război și că amenințarea teroristă rămâne iminentă. Deoarece nu au existat atrocități cu bombe pe străzi sau gazări în masă în metroul londonez, publicul a rămas protejat de ceea ce politicienii insistă să numească o falsă senzație de siguranță și fie nu acordă importanță avertizărilor guvernului și poliției, fie respinge aceste avertizări, considerându-le minciuni sau vorbe goale. Mulți dintre noi își mai amintesc încă violențele campaniei cu bombe purtate de IRA (și unii dintre noi au luat contact direct cu ele), dar chiar și amintirile noastre se estompează în timp, lăsând în urmă un aer de indiferență față de actuala amenințare teroristă.

În Statele Unite, politicieni, printre care și președintele Statelor Unite sau secretarul apărării Donald Rumsfeld, au vorbit despre teroriști Al Qaeda înarmați, umblând în libertate prin Europa, și au făcut cumva o legătură între aceasta și situația din Irak, pentru a-și justifica decizia de a porni un război. Dar publicul britanic nu a avut niciun fapt pe baza căruia să-și formeze o opinie. Motivul pentru această ignoranță generală în ceea ce privește situația actuală a terorismului din Marea Britanie îl constituie seria de trei procese corelate care se aflau în derulare la Old Bailey (Curtea Penală Centrală) și care s-au încheiat de-abia în primăvara lui 2005. Dacă mass-media ar fi avut acces la detalii înainte de încheierea procesului, acesta nu s-ar mai fi putut desfășura corect. Lordul Cancelar a *emis un ordin pentru toate cele trei procese, care a interzis orice* comentariu legat de aceste subiecte. Abia în aprilie 2005 a fost recunoscut în mod public că, între anii 2004 – 2005, Curtea Penală Centrală din Londra a fost într-o permanentă, stare de alertă crescută, din pricina afirmațiilor referitoare la planuri teroriste musulmane care au pătruns în sistem. S-au strâns tot mai multe dovezi care demonstau că teroriștii plănuiau atacuri în toată capitala britanică, cu ajutorul explozibililor, al cocktailurilor cu gaze otrăvitoare, al ricinei și al altor substanțe chimice toxice.

Puținii privilegiați care au urmărit în Old Bailey procesul intentat teroristului fanatic Kamel Bourgass și complicilor lui s-au întrebat probabil de ce anume e nevoie pentru a convinge publicul britanic că se confruntă cu un mare pericol.

În primele două procese, au fost aduse acuzații împotriva a opt bărbați inculpați, dar au mai fost implicați cel puțin încă alți șase, care n-au fost niciodată prinși, și câțiva activiști, ale căror, detalii rămân necunoscute. Unii dintre acuzați erau teroriști bine pregătiți, având legături cu taberele de antrenament Al Qaeda din Afghanistan; ei frecventau moscheea din Finsbury Park din nordul Londrei, folosind-o drept centru de comandă pentru a purta războiul pe teritoriul britanic. Procesele nu numai că au dezvăluit pericolele cu care s-a confruntat publicul britanic după 9/11, dar au arătat în detaliu și incapacitatea agențiilor de apărare trimise să ancheteze și să-i aresteze pe teroriștii implicați.

Nigel Sweeney, procuror al Coroanei în procesul Bourgass, a prezentat dovezi care demonstau fără putință de tăgadă că moscheea Finsbury Park era un centru terorist unde erau copiate și distribuite fundamentalistilor din întreaga țară rețete pentru ricină, gaze otrăvitoare și explozibili. Rețetele au fost descoperite inițial în Kabul, în timpul Războiului din Afghanistan, și nu erau altceva decât niște încercări școlarești de a fabrica otravă. Detalii ale celulelor teroriste, inclusiv fotografiile, au fost descoperite după ce MI5 a primit un pont și au fost folosite ca dovezi. La primul proces, în boxa acuzaților au fost Kamel Bourgass, Mouloud Sihali, David Aissa Khalef, Sidali Feddag și Mustapha Taleb. Acuzațiile care le-au fost aduse au fost de complicitate la crimă și plănuirea unor acțiuni periculoase la adresa populației între 1 ianuarie 2001 – 23 ianuarie 2002. Toți, cu excepția lui Bourgass, au fost declarați nevinovați de acte teroriste. Bourgass era un tânăr de 27 de ani, licențiat în științele naturii, și un produs al taberelor de antrenament Al Qaeda din Afghanistan, a cărui singură infracțiune anterioară fusese o condamnare pentru că furase dintr-un magazin trei perechi de blugi, în iulie 2002. Juraților le-au trebuit 15 ore ca să-l condamne pe Bourgass

pentru moartea polițistului Stephen Oake, pentru tentativă de omucidere împotriva a doi ofițeri din Divizia Specială și pentru vătămarea corporală premeditată a sergentului de poliție Paul Grindrod. A fost condamnat la închisoare pe viață, plus alți 17 ani, în paralel, pentru acte teroriste. Judecătorul procesului a recomandat ca Bourgass să petreacă cel puțin 30 de ani în închisoare, înainte de a fi putea fi eligibil pentru eliberare condiționată. În timp ce îi citea sentința, judecătorul a comentat că, 30 de ani e cea mai lungă condamnare pe care o poate da, deoarece noua lege penală, Criminal Justice Act, nu fusese încă promulgată. Dacă ar fi putut, ar fi ordonat ca Bourgass să fie închis pentru tot restul vieții.

Acuzații în cel de-al doilea proces au fost: Khalid Alwerfeli, Samir Asii, Mouloud Bouhrama, Kamel Merzoug și un al cincilea bărbat, Mohamed Meguerba, care a încălcat cautiunea și a fugit în Algeria. Toți, cu excepția lui Meguerba, au fost absolviți de acuzația de terorism, dar condamnați pentru încălcarea legii imigrării. Cel de-al treilea proces nu a mai fost intentat. Nigel Sweeney a declarat în fața instanței: „Cel puțin zece musulmani ale căror nume sunt cunoscute, împreună cu persoane necunoscute, plănuiau să provoace moartea, rănirea sau înspăimântarea populației britanice printr-un Jihad (război sfânt)”. Toți erau imigranți ilegali din Algeria, trăind în locuințe secrete în Manchester, Londra, Doncaster și Boumemouth. Punerea la cale a unui atac terorist „spectaculos” a început în ianuarie 2001, dar descoperirea care a salvat Londra de violențe grave n-a avut loc decât doi ani mai târziu, în ianuarie 2003, când ofițeri antitero din Divizia Specială au percheziționat un apartament de două camere din Wood Green Lane (nordul Londrei) și au descoperit o fabrică de arme chimice.

Otrăvurile și gazele provoacă spaimă și panică în rândul populației. În apartament, ofițerii Diviziei Speciale au găsit ingredientele, echipamentul și instrucțiunile necesare pentru a prepara, printre alte otrăvuri mortale, ricină, toxină botulinică (care cauzează botulism) și „otrava cărnii putrezite”, care e la fel de oribilă pe cât sună. „Otrava cărnii putrezite” este

considerată de o mie de ori mai puternică decât gazele neuroparalitice și e nevoie de doar o cantitate infimă ca să provoace moarte instantanee. Presupusa experiență a lui Bourgass cu otrăvurile a fost subliniată și de descoperirea unor rețete de preparare a otrăvii cu nicotină, otrăvii cu cartofi și a cianurii. Un detectiv a descris-o drept fabricare „artizanală” de bombe care nu necesită decât cunoștințe elementare de chimie și în care sunt folosite ingrediente de prăvălie. De fapt, totul dădea impresia de diletantism.

Toate materiile prime erau ușor de obținut. Pachetele de ingrediente găsite în apartament includeau semințe de ricin, materia primă pentru ricină, una dintre cele mai ușor de fabricat și în același timp una dintre cele mai eficiente otrăvuri, ceea ce o face o resursă ideală pentru teroriști. Poliția a mai descoperit semințe de măr și sămburi de vișine din care poate fi extrasă cianura. Cianura este o substanță mortală, folosită în lagărele de exterminare naziste în timpul celui de-al Doilea Război Mondial (deși este nevoie de cantități foarte mari de semințe de măr și sămburi de vișine pentru a se obține o cantitate letală). Investigatorii au mai găsit acetona, care este folosită în procesul chimic de extragere a otrăvii din semințe, și echipamente folosite pentru a transforma otrava lichidă în gaz. Otrava cu nicotină a fost descoperită într-un borcan. S-au găsit copii cu instrucțiuni despre folosirea obiectelor casnice de zi cu zi pentru a fabrica explozibili, cum ar fi bombe fumigene sau bombe-bliț, precum și detonatoarele care le însoțesc. Diagrame cu circuite potrivite pentru detonatoare și bombe improvizate, folosite în mod curent de teroriștii din întreaga lume, zăceau de asemenea în apartament. Cele mai multe dintre materiale puteau fi cumpărate prin internet. Au fost găsite și câteva dintre ustensilele de bază ale unui chimist, cum ar fi pistil și mojar, măcinător de cafea, mănuși de cauciuc, hârtie sugativă, termometre, retorte, baloane și pâlnii.

A devenit curând evident faptul că apartamentul din Wood Green era o fabrică de arme chimice, iar formulele, scrise în arabă, aveau o bază științifică și fuseseră fotocopyate la



moscheea din Finsbury Park, înainte de a fi distribuite în rândul comunității musulmane ostile. Instrucțiunile fuseseră scrise de Bourgass și erau pline de amprente ale lui. Când Mustapha Taleb a fost arestat, Divizia Specială a găsit în posesia lui și un CD pe care erau ridicate în slăvi beneficiile bombardărilor folosind tehnologia modernă. Pe el erau incluse instrucțiuni despre asamblarea și montarea dispozitivelor de cronometrare.

Mare parte din ceea ce se știe despre Bourgass a venit din partea lui Mohamed Meguerba, care a fost arestat de poliția algeriană curând după ce a fugit din țară, încălcând condițiile de cauțiune impuse în Marea Britanie. A fost supus unor interogatorii și a început curând să furnizeze detalii despre celulele teroriste care operau în Londra și Manchester, precum și despre alte activități care se desfășurau în moscheea din Finsbury Park, dând în vileag tot ce știa despre Al Qaeda. Mărturisirea lui Meguerba și declarația de 27 de pagini, obținute aproape sigur prin tortură, au fost imediat transmise serviciilor secrete britanice. Le-a spus anchetatorilor că a făcut parte dintr-o grupare care fabrica arme chimice improvizate și plănuia atacuri împotriva persoanelor civile, „inclusiv evrei”, pe teritoriul britanic. Obiectivul era să răspândească spaima și panica. A declarat că planurile includeau mînjirea cu lichide și paste otrăvitoare a mașinilor și a mânerelor ușilor din nordul Londrei. Meguerba a susținut că ar fi umplut două borcane cu ricina pe care o fabricase și că i-ar fi dat otrava unui bărbat pe nume Nadir, din apartamentul din Wood Green Lane. Poliția care a percheziționat apartamentul a descoperit planurile, dar nu era nicio urmă de borcane cu ricină.

Dacă ați clona un terorist musulman, cel mai probabil l-ați face după chipul și asemănarea lui Kamel Bourgass. Bourgass venise în Dover din Calais, în remorca unui camion, în ianuarie 2000, și mersese direct la moscheea din Finsbury Park, unde i s-a spus să ceară azil la Centrul de Imigrări din Croydon. Pentru prima solicitare de azil, din februarie 2000, și-a dat numele de Nadir Habra și a declarat că s-a născut în 1973. A dat moscheea ca adresă și a pretins că nu deține un

pașaport. A fost nevoie de 20 de luni ca aplicația lui să fie procesată și respinsă. Apelul lui împotriva deciziei a fost respins în decembrie 2001. Anticipând rezultatul, Bourgass/Habra nu s-a prezentat la apel, evitând astfel arestarea și deportarea, și a dispărut în mijlocul comunității musulmane din nordul Londrei.

Ascunzându-se de justiție pe străzile lăturalnice din Tottenham și Edmonton, el și-a schimbat identitatea și a făcut rost de un pașaport francez fals. Când a fost oprit de polițiști, în iulie 2002, s-a dat drept Kamel Bourgass, un marocan născut în 1975. Poliția antitero și Divizia Specială n-au fost în stare să-l identifice drept Nadir Habra, dar au decis totuși să-i urmărească pe Bourgass și tovarășii săi. Apartamentul din Wood Green Lane a fost descoperit în timpul unei anchete separate asupra unei rețele de fraudă extinse în toată Europa, despre care se credea că strângea fonduri pentru Al Qaeda.

În noiembrie 2002, poliția a efectuat arestări în întreaga parte de nord a Londrei și l-a reținut pe Mouloud Sihali, specializat în a face rost de cazare și acte de identitate pentru cei în căutare de azil. În apartamentul lui din Ilford au fost găsite cinci pașapoarte false, dintre care unul cu poza unui suspect terorist dat în urmărire. Polițiștii au găsit și detaliile unei adrese din Thetford, unde l-au arestat pe David Khalef. Sihali și Khalef au fost condamnați pentru falsificare de pașapoarte, dar nu au fost puși sub acuzare conform Legii împotriva terorismului. Și totuși, în servieta lui Khalef au fost găsite documente în arabă, pe care erau imprimate instrucțiuni despre cum să fabrici otravă și explozibili. Cercetătorii de la laboratoarele Port Down au testat instrucțiunile pentru otrăvuri și au confirmat că ar putea fi folosite pentru a produce doze letale de toxine. Descoperirea faptului că în Londra trăiau imigranți care aveau cunoștințele și capacitatea de a produce otrăvuri mortale, ce ar putea fi folosite într-un atac asupra capitalei, a avut un impact major asupra forțelor de securitate, iar suspiecții au fost ținute sub supraveghere, luni de-a rândul, de către MI5. Bourgass, pe cale de a deveni cel mai căutat om din Marea Britanie, a

părăsit apartamentul din Wood Green Lane cu câteva ore înainte ca poliția să percheziționeze imobilul. Amprente și fotografii de pașaport ale sale au fost găsite în apartament și transmise tuturor forțelor de poliție. Dar poliția nu avea idee în acel moment unde se află sau, și mai grav, cine e de fapt. Bourgass a ajuns până în Boumemouth, de unde s-a hotărât să ia cursa de noapte de la Weymouth până în Manchester. Avea nevoie disperată de un pașaport fals, astfel încât s-a îndreptat spre o locuință secretă din Crumpsall Lane, o stradă liniștită din partea de nord a orașului. Aceasta era casa unui libian, Kalid Alwerfeli. Decizia aceasta i-a fost fatală lui Bourgass, deoarece poliția plănuise deja să percheziționeze imobilul. Lațul începea să se strângă.

Descoperirea apartamentului din Wood Green Lane a fost în mod evident o lovitură importantă pentru serviciile de securitate. Ea a fost rezultatul urmăririi unui pont primit de MI5 din partea poliției antitero pariziene. Clădirea fusese monitorizată de mult timp, iar bărbații care o foloseau fuseseră filmați și urmăriți. Cu toate acestea, în vreme ce prima razie păruse a fi o lovitură grea dată terorismului din Marea Britanie, operațiunea ulterioară a poliției, cunoscută ca „Operațiunea Salt”, a fost un dezastru. La ora patru și jumătate în după-amiaza zilei de 14 ianuarie 2003, apartamentul 4 de la numărul 4 de pe Crumpsall Lane a fost percheziționat de ofițerii Diviziei Speciale, de funcționari de la Imigrări și de o Unitate de Ajutor Tactic (UAT) formată din trei oameni și specializată în pătrunderea în locuințe și securizarea acestora. Sarcina acestei unități era de a pătrunde cu forța în apartament. Se bănuia că principala țintă a acestei razii, Sofiane Mihoubi, a cărui arestare fusese ordonată de către ministrul de interne David Blunkett, ca urmare a unei informații primite de MI5, se afla în apartament. Cel de-al treilea locatar era Khalid Alwerfeli, libianul de 31 de ani care închiriasse apartamentul. În noiembrie 2002, lui Alwerfeli i se acordase permisul de ședere pe termen nelimitat pentru a rămâne în Marea Britanie. Era singurul membru al celei care nu era algerian. Intrase în Anglia în 1999, folosind un fals act

francez de identitate.

Razia din Crumpsall Lane a fost plănuită imediat după descoperirea otrăvurilor și a explozibililor din Wood Green Lane. Poliția și funcționarii de la Imigrări implicați habar n-aveau cât de mare era pericolul care-i aștepta. Privind retrospectiv, demersul lor nu poate fi descris decât ca accidental. În procesul de la Old Bailey, Nigel Sweeney a enumerat ceea ce el a numit eufemistic „neajunsurile poliției” în această operațiune, care a implicat 23 de ofițeri. El a declarat în fața instanței: „N-a existat nicio evaluare a riscului, niciun ordin operațional scris, nicio cercetare preliminară a incintei, pentru a determina poziția exactă a apartamentului, nicio informație asupra persoanelor care se găseau înăuntru și nici măcar dacă Bourgass se afla acolo, niciun instructaj operațional serios înaintea raziei, nicio transparență în ceea ce privește rolul fiecărui ofițer, nicio înțelegere de ansamblu asupra importanței țintelor, niciun echipament de arestare pentru imobilizare, nu au existat comunicări bine planificate sau veste antiglonț”. Unicul instructaj operațional a avut loc într-un garaj al secției de poliție Collyhurst, în timp ce se schimbau turele de serviciu. Supravegherea pare să fi fost făcută în grabă, probabil fiindcă nu a existat destul timp ca să fie instalate camerele și analizate riscurile. Colac peste pupăză, între ofițerii Diviziei Speciale implicați în razie și inspectorul-șef care conducea operațiunea exista o oarecare tensiune, iar rețeaua de telefonie mobilă a Diviziei Speciale a cedat în timpul raziei, obligându-i pe ofițeri să-și folosească telefoanele personale. Un nou eșec adăugat pe listă: Mohamed Meguerba, jucător-cheie în această conspirație, a fost arestat, dar eliberat pe cauțiune, putând astfel să fugă în Algeria, unde a fost arestat mai târziu.

Poate părea evident că, atunci când ținta este o celulă teroristă, e nevoie de precauții speciale din partea ofițerilor de poliție implicați și că, înainte de toate, poliția trebuie să se asigure că toată lumea găsită la fața locului este imobilizată cât mai repede. Dar nimeni nu s-a asigurat de toate acestea. Ulterior, polițiștii au declarat că Bourgass părea liniștit și că ei

au ținut să nu distrugă eventualele probe de pe mâinile și corpul lui. Poliția le-a ordonat locatarilor să se dezbrace, apoi să-și pună hainele în pungi și le-au dat suspectilor să îmbrace salopete albe. Ofițerii Diviziei Speciale nu purtau veste antiglonț și, timp de 90 de minute după ce au intrat în casă, Kamel Bourgass a fost lăsat să stea fără cătușe. Curelele de plastic care se folosesc în mod normal pentru a lega mâinile suspectilor rămăseseră la secția de poliție.

Bourgass a declarat un nume fals în fața polițiștilor și a funcționarilor de la Imigrări care au intrat în apartament, însă a fost recunoscut datorită fotografiilor furnizate de serviciile de securitate. Poliția știa că documentele incriminatoare găsite în Wood Green Lane erau pline de amprentele lui Bourgass și că acesta era un important suspect de terorism. Era evident că el se afla într-o situație disperată și că arestarea lui ar fi echivalat cu ani grei de închisoare, în cazul în care n-ar fi găsit o cale de scăpare. Cu toate acestea, el a fost condus în dormitor de către un polițist în uniformă pe nume Fleming, care era la prima sa operațiune teroristă în cadrul UAT. Sofiane Mihoubi se afla în aceeași cameră și stătea pe celălalt pat, unde era păzit de polițistul Stephen Oake. Aiwerfeli era în camera de zi, sub paza a doi bărbați din Divizia Specială. Mai mulți polițiști și ofițeri de la Imigrări se aflau pe palierul din afara apartamentului, iar alți câțiva în camera de zi, ocupați cu făcutul pozelor și cu adunatul dovezilor.

Bourgass rămăsese pasiv, neopunând nicio rezistență. Aștepta momentul când ar fi simțit atenția celor care-l păzeau slăbind și eventual cedând. E genul de bărbat puternic, vânjos, bine clădit, și avea șansa de a ataca prin surprindere, atuul disperării și al familiarității cu mediul. Era 5.45 p.m. Când, fără nicio avertizare, Bourgass s-a ridicat de pe pat, l-a lovit puternic pe polițistul Fleming în vintre, a fugit în bucătărie, a luat un cuțit cu o lamă de 12 centimetri din suportul de uscare și a început să înjunghie pe toată lumea din apropiere. „Era gata să ucidă pe oricine i-ar fi stat în cale”, a declarat Nigel Sweeney la proces. În timpul luptei, polițistul Oake, tatăl a trei copii și predicator laic în timpul liber, a fost înjunghiat de

patru ori în piept. Trei dintre lovituri i-au fost fatale. O lovitură i-a străpuns inima, iar alte două i-au perforat plămânii. Alți doi ofițeri ai Diviziei Speciale au fost răniți în timpul atacului. Unul din ei a fost înjunghiat de două ori în braț, iar un detectiv al cărui nume nu a fost menționat, dar care în timpul procesului a fost botezat John, a fost înjunghiat în piept, în lateral și în spate. Sergentul Paul Grindrod din cadrul UAT a fost înjunghiat în spate și în picior. Bourgass a reușit să nimerească în total 13 lovituri în timpul atacului său turbat.

Consecințe teribile ale descoperirii unei fabrici teroriste de bombe, pe lângă moartea lui Stephen Oake, au fost și conștientizarea faptului că serviciile britanice de securitate nu sunt îndeajuns de antrenate sau capabile să facă față teroriștilor hotărâți, nici măcar acelor incompetenți precum Bourgass. Deși poliția și serviciile de securitate au primit toate informațiile cu privire la amenințarea teroristă, acestora le-a lipsit capacitatea să le analizeze și să le folosească în mod constructiv, astfel încât să-i aresteze rapid și eficient pe toți suspecții. Bourgass era după o încercare nereușită de a obține azil, era imigrant ilegal și, evident, un bărbat instabil și periculos. Deși a fost prins, condamnat și trimis la închisoare, simplul fapt că a petrecut atâția ani plimbându-se nestingherit prin Marea Britanie și Europa trebuie să fi fost o încurajare pentru ceilalți extremiști care erau deja în Marea Britanie. Există dovezi care arată că Bourgass a fost de fapt membru al unei celule teroriste conduse de un algerian, Abu Doña. Se știe că, în 1998, Doña, cunoscut și ca „Doctorul”, „Rachid” sau „Amar Makhulif”, a condus o rețea de asemenea celule. Se crede că a fost membru al „Grupării Salafiste pentru Apel și Luptă”, care a comis nenumărate atrocități în Algeria și care a fost angajată să organizeze tabăra de antrenament Khalden din Afghanistan, unde erau instruiți membrii nord-africani și mujahedini. Tabăra pregătea sute de teroriști, iar Osama Bin Laden era un vizitator frecvent, potrivit celor care s-au antrenat acolo și au fost mai târziu arestați. Mulți dintre ei au fost trimiși să lupte în Cecenia, iar alții au fost trimiși să

lucreze sub acoperire în Occident.

Doña s-a stabilit în nordul Londrei, unde se găsește o comunitate algeriană puternică, alcătuită din cei care au scăpat de luptele acerbe de la ei din țară. Potrivit judecătorului Ouseley, care l-a condamnat pe unul din complicii lui Doña, „prezența sa, la fel ca a lui Bourgass, a mărit coeziunea cauzei extremiste algeriene în Marea Britanie”. La sfârșitul anului 2000, în urma unei informații primite de la ofițerii MI6, care au interceptat un apel din partea lui Doña, polițiștii germani au făcut o razie la o adresă din Frankfurt, unde au descoperit patru bărbați, dar și echipament de fabricat bombe și o cameră de supraveghere a pieței Strasbourg. Trei dintre bărbații din apartament erau cetățeni britanici. Toți au fost arestați și trimiși ulterior la închisoare. Doña, care călătorea cu un pașaport fals, a fost arestat la Heathrow în februarie 2001, în timp ce încerca să prindă un zbor spre Arabia Saudită. Apartamentul său din Edmonton s-a dovedit a fi o sursă bogată de dovezi acuzatoare, incluzând instrucțiuni de fabricare a bombelor și pașapoarte false. Doña rămâne în custodie la închisoarea Belmarsh și se apără pentru a nu fi extrădat în Statele Unite. Nimeni nu pare a ști dacă rețeaua de teroriști a lui Doña își continuă activitatea sau dacă s-a dizolvat, odată cu arestarea lui Bourgass. Activiștii din taberele Al Qaeda simt antrenați să se descurce singuri și să continue, dacă e nevoie, fără alți membri activi.

Ahmed Ressay, terorist condamnat care se află închis în Statele Unite, după ce a plănuțit un atac cu bombă asupra aeroportului din Los Angeles, era în strânsă legătură cu Doña înainte de arestarea sa. Ressay a fost prins în Seattle purtând arme și explozibili pentru a fi folosiți în atac. Amenințat de o condamnare la 130 de ani de închisoare, el a decis să coopereze cu FBI-ul. Djamel Beghal din Leicester, un alt membru al celulei, a fost arestat în Dubai în 2001, sub acuzația de plănuire a unui atac asupra Ambasadei Statelor Unite din Paris. El rămâne închis într-o închisoare franceză. Un fost fotbalist profesionist tunisian, Nizar Trabelsi, care s-a

antrenat și el cu Doña în Afghanistan, a fost arestat în Bruxelles, având asupra lui echipament pentru fabricarea bombelor; se bănuiește că el se oferise voluntar pentru un atac sinucigaș cu bombă. Trabelsi plănuise să bombardeze baza militară aeriană NATO Kleine Brogel. După introducerea în 2001 a Legii puterilor de urgență, mai mulți bărbați suspecti de a fi membri ai rețelei lui Doña au fost reținuți. Noul conducător al rețelei, Kadre, a fost arestat la Londra, în timp ce se îndrepta – după cum bănuiește poliția – către Bourgass, pentru a-l activa și a-i da o mână de ajutor în complotul cu ricină. Bourgass a fost reținut două luni mai târziu, iar arestarea lui marchează probabil sfârșitul acelei celule. Privind retrospectiv, planul de a folosi ricină și „otrava cărnii putrezite” (cu sonorități atât de dezgustătoare) pare excentric, dar el ar fi putut să aibă loc și ar fi creat cu siguranță o panică îngrozitoare în capitală. Ar fi făcut de asemenea să crească tensiunile dintre musulmanii care respectă legea și comunitățile în care ei trăiesc.

Procesul lui Bourgass pune câteva probleme grele MI5-ului și în special Serviciului de Imigrări. De mulți ani, agențiile franceze de spionaj avertizau serviciile secrete britanice că algerieni implicați în atrocitățile din propria țară și nu numai se strecurau în Marea Britanie și cereau azil. Dar nu s-a făcut mai nimic în această privință. Autoritățile britanice și-au justificat inacțiunea spunând că n-au avut nicio dovadă de încălcare a legii. Atacul asupra turnurilor gemene și noua legislație împotriva terorismului au schimbat, după cum era și firesc, toate acestea și au acaparat atenția serviciilor secrete. Din acel moment, serviciilor franceze de spionaj li s-a acordat mai mult credit și se pare că de atunci a fost ținută sub supraveghere comunitatea algeriană. Trebuie totuși precizat că „supravegherea” n-a fost prea satisfăcătoare. În ciuda celor declarate, Bourgass putea să vină și să plece după bunul plac, călătorind în Europa cu acte false și schimbându-și în mod constant identitatea, fără a atrage atenția autorităților. Pretinsa creștere a supravegherii n-a avut un impact prea mare, iar Serviciul de Imigrări a demonstrat o relaxare



îngrozitoare. Se pare că se bănuia de mult timp că moscheea din Finsbury Park ar fi folosită ca adăpost de către imigranții ilegali și ca loc de obținere a documentelor de identitate false, dar a fost pusă sub investigație abia atunci când putea fi prea târziu. Algerienii cu care se asociase Bourgass nu au fost opriți la niciunul dintre porturile sau aeroporturile prin care au trecut. Există aproape o sută de milioane de intrări în Marea Britanie în fiecare an și, desigur, numai un mic număr e reprezentat de teroriști. Totuși, există foarte puțini angajați disponibili la Imigrări care să verifice cine trece și să ia măsuri în privința vizitatorilor suspecti. Pare greu de crezut acum, dar în 2002, în Londra nu erau ofițeri ai Serviciului de Imigrări de serviciu după ora cinci.

Americanii, cu granițele lor poroase din nord, sud și est, luptă cu imigrația la asemenea proporții cu mult timp înaintea britanicilor. Orice plan care are o șansă cât de mică de a ține indivizii nedoriti în afara țării trebuie să poată asigura paza coastelor sale enorme și a frontierelor, precum și a spațiului său aerian. Atacul de la 11 septembrie a inspirat un apel național pentru întărirea securității frontierelor și, cel mai important, a cerut un răspuns la întrebarea: „Cum împiedicăm alte atacuri?” Prima decizie luată, o consecință imediată a dezastrului, a fost ca toate aeronavele comerciale care zburau să fie aduse la sol pe cel mai apropiat aeroport, astfel încât inamicul să nu poată folosi văzduhul. Decizia avea sens din punct de vedere operațional, deoarece, la momentul respectiv, se aflau în aer numeroase aeronave încărcate cu armament militar și exista un mare risc ca o cursă aeriană nevinovată să fie doborâtă de vreun pilot de luptă mai nervos și nerăbdător să apese declanșatorul. Dar asta implica și faptul că tuturor cetățenilor americani care respectă legea le era interzis să călătorească cu avionul. Să oprești rețeaua de trafic aerian e ca și cum ai recunoaște că nu o poți apăra, ceea ce face mai mult rău poziției țării decât chiar teroriștii de la care a pornit totul. Numai în 2002 au fost 8 789 123 de decolări civile în Statele Unite – adică o medie de 24.000 de zboruri pe zi. Un total de 539 883 008 pasageri s-au înregistrat în aeroporturile

americane în 2002, ajungând la aproape un milion și jumătate de pasageri în fiecare zi a anului, în Statele Unite, transportul aerian este o industrie enormă și vitală, bazându-se pe sute de aeroporturi comerciale. E clar că este imposibil să previi orice penetrare a perimetrului aeroportului fără a restricționa puternic fluxul zilnic al traficului aerian.

Administrația Bush era perfect conștientă de vulnerabilitatea Statelor Unite la un atac și de cât de ușor poate fi paralizată rețeaua de transport. Sunt vreo duzină de ținte care, dacă ar fi atacate și grav deteriorate, ar lăsa foarte repede națiunea în impas. De exemplu, râul Mississippi curge din Minnesota până în Golful Mexic și este, normal, străbătut de un număr mare de poduri. Cel mai încărcat trafic rutier și feroviar este limitat, totuși, la vreo 20 de puncte de trecere. Dacă doar șase dintre aceste puncte de trecere ar fi scoase din acțiune, drumul de la est la vest și traficul feroviar ar suferi întârzieri enorme, iar economia Statelor Unite ar fi paralizată. O problemă asemănătoare există în Manhattan, care, într-o zi obișnuită a săptămânii, are o populație lucrătoare de aproape trei milioane de oameni. Există numai șase poduri și patru tunele ca să ajungi sau să pleci de pe insulă. Un atac chimic sau biologic ar putea lăsa insula izolată, provocând panică în masă; ar cauza întreruperea transmisiunilor TV și a sistemelor financiare din Statele Unite și ar putea aduce disperare națională. Daune grave ar putea fi aduse industriei petroliere chiar și numai blocând Canalul Naval Houston, de-a lungul căruia petrolul este transportat pe vase din Golful Mexic, pentru a alimenta rafinăriile din Pasadena. O navă-cisternă scufundată ar cauza instantaneu un deficit de petrol în Statele Unite. Din cauza progresului, țările industriale sunt întotdeauna vulnerabile la atacuri cu bombă în centrale electrice, nave sau clădiri guvernamentale. După distrugerea turnurilor gemene, administrația n-a avut ce face altceva decât să avertizeze asupra eventualelor atacuri viitoare și să solicite o legislație dură.

Imediat după atacul asupra turnurilor gemene, serviciile de securitate și de imigrări au primit sarcina de a crea un nou

program de monitorizare a pasagerilor, pentru a preveni repetarea unei asemenea atrocități. Identificarea unui număr mic de potențiali teroriști din cele zece milioane de mișcări zilnice ale pasagerilor necesită munți de informații, din care potențialii teroriști trebuie identificați și separați de majoritatea covârșitoare a oamenilor care nu reprezintă niciun fel de amenințare la adresa statului. Trebuie creat un program permanent, care să examineze electronic fiecare rezervare a pasagerilor care intră sau ies din aeroporturile americane civile, să identifice călătorii și să creeze un profil pentru fiecare călător. Anomaliile sau profilurile care nu se încadrează în criteriile stabilite de agențiile de spionaj ar fi verificate, pentru a se decide dacă indivizii identificați aparțin sau nu unei organizații teroriste. Acesta este un plan uriaș și care ar putea avea urmări dezastruoase.

Programul CAPPSII era atât de sensibil și secret, încât în timpul alegerilor prezidențiale din 2004 a trebuit să fie abandonat discret și temporar. Cheia programului o reprezintă implicarea unor companii ca Acxiom Corporation, o companie ce analizează scorurile de credit și deține detalii despre aproape orice persoană din Statele Unite sau Europa. Partenerii săi, NC Software, sunt specializați în detectarea riscurilor și au creat un software pentru analize complexe și detaliate ale tranzacțiilor comerciale simple. Aceste companii pot procesa simultan miliarde de înregistrări și au experiență în lucrul cu industria de asigurări, cu emitenții de cărți de credit și cu companiile de telefonie. Sunt experți în detectarea fraudelor înainte și după ce acestea au loc.

O mare parte din industria de procesare a datelor și-a oferit serviciile gratis agențiilor americane de impunere a legii încă de când turnurile gemene fumegau. În doar câteva ore s-au primit cereri de analiză a bazelor de date din partea FBI-ului, a serviciilor secrete și a poliției. Lexisnexis, care este uneori confundată cu o agenție de resurse legale sau de monitorizare a presei, a sărit și ea imediat în ajutor. Lexisnexis este de fapt o subsidiară a editurii-gigant britanice Reed Elsevier, care are sediul în Londra, dar și subsidiare americane. Lexisnexis

deține rapoarte detaliate despre milioane de persoane, familii și companii, achiziționate inițial de la arhivele publice și conținând numere de la Protecția Socială, date de naștere și multe altele. La început, compania a funcționat drept bibliotecă legală a Fiscului american și a creat un sistem de telecomunicații pentru a ajuta la o funcționare mai rapidă a serviciului pe care Fiscul îl pune la dispoziția clienților săi. La sfârșitul anilor 1990, Lexisnexis a cumpărat o afacere intitulată Risk-Wise, care evaluează automat neregulile și potențialul de risc. Lexisnexis putea acum să acorde o „notă” persoanelor, bazată pe factori precum probabilitatea lor de angajare, experiența sau nivelul lor de competență într-un anumit tip de muncă. Capacitățile companiei Lexisnexis erau ideale pentru ca administrația să încerce să evalueze potențialul de risc al unui dezastru asemănător cu cel care tocmai lovise Statele Unite.

În prezent, Lexisnexis deține 16.000 de baze de date, are trei milioane de abonați și folosește 36.000 de surse de informații, cum ar fi arhive publice, decizii ale curților judecătorești, rezultate financiare, evaluări de credite și chiar zvonuri. Lucrează pentru serviciile de spionaj, pentru presă și pentru cei din sistemul judiciar. Când vrei să verifici dacă o persoană e potrivită să lucreze cu copiii, Lexisnexis îți va furniza un portret de ansamblu al applicantului, incluzând eventuale condamnări penale și aproape orice altceva te-ar putea interesa. Sistemele companiei procesează și analizează informații despre milioane de persoane, răspunzând la o diversitate de criterii. Ca urmare a haosului de după dezastrul din New York, Lexisnexis a fost de acord să înființeze un grup operativ, „Dezastrul central” în Washington DC, și să-și pună bazele de date la dispoziția tuturor agențiilor de impunere a legii. Atmosfera dominantă în acel moment era că ar trebui făcut tot posibilul ca toți cei vinovați de această atrocitate să fie prinși și trimiși la pușcărie. Aceasta nu numai din cauza dorinței de răzbunare, dar și fiindcă autoritatea și independența Statelor Unite trebuiau apărate cu orice preț. Nu există nicio limită a cooperării pe care industria comercială

era dispusă s-o ofere. Agențiile furnizoare de date știau că ajutorul lor era nu numai vital, dar și o investiție în bunăvoință care le va aduce profit în viitor. Peste noapte, informațiile colectate în mod profesionist au devenit un bun neprețuit. Pentru unii, tragedia de la 11 septembrie a devenit, în mod evident, o oportunitate de afaceri neprețuită.

Sistemele și computerele Lexisnexis au fost conectate imediat la computerele guvernului și la bazele de date ale serviciilor de spionaj. Nu e nicio surpriză că una dintre prioritățile companiei era să-și folosească tehnologia de evaluare a riscurilor ca metodă de analiză a credibilității identităților date de cetățenii neamericani care s-au înscris la cursuri ale școlilor de aviație. Administrația Bush a elaborat o listă cu aproape 20.000 de suspecti de terorism, având la bază tot felul de criterii îndoielnice, iar Lexisnexis a primit sarcina de a-i monitoriza constant. Majoritatea numelor de pe listă nu se făceau vinovate de niciun delict, dar tehnicile companiei au înregistrat câteva succese notabile, identificând, de exemplu, o casă din Florida, pe care teroriștii care deturnau avioane o împărțeau când participau la cursurile de pilotaj.

Lexisnexis era conștientă de temerile guvernului american privind faptul că era vorba de o companie britanică, așa că a depus toate eforturile ca să fondeze în 2003 o nouă subsidiară, denumită Lexisnexis Special Service. Lucrul acesta a fost pe placul avocaților guvernamentali, al serviciilor secrete și al agențiilor de impunere a legii, dar și al administrației Bush, iar compania a primit imediat permisiunea să lucreze cu cele mai delicate secrete ale Statelor Unite. Noua companie a devenit responsabilă cu Proiectul Securității Aviatice, CAPPSII, la care a început să lucreze împreună cu o nouă agenție guvernamentală, numită Oficiul Național de Evaluare a Riscurilor. Din acest moment, Lexisnexis a început să ceară bani pentru serviciile oferite.

În 2003, organizațiilor pentru libertăți cetățenești au început să le ajungă la urechi zvonuri despre CAPPSII și despre conceptul de a aplica evaluări ale riscurilor și amenințărilor tuturor aeronavelor de transport, pasagerilor,

aeroporturilor și zborurilor efectuate în Statele Unite, precum și ale fiecărui pasager care zboară în sau din Statele Unite. Un grup denumit Centrul pentru Intimitatea Datelor Electronice (EPIC) a fost foarte deranjat de ceea ce auzea. Acum pare uimitor faptul că Departamentul de Stat și Departamentul Securității Interne au omis să împărtășească informațiile despre sistemul CAPPSII grupurilor de presiune ce apără drepturile cetățenești sau mass-mediei, deoarece era un subiect ce nu putea să nu iasă la lumină, iar când acest lucru s-ar fi întâmplat, răspunsul ar fi fost pe măsură. Și exact asta s-a întâmplat. Guvernul a fost prins punând la cale cel mai amplu sistem de supraveghere internă impus vreodată publicului american, fără să dezvăluie vreun detaliu organizațiilor ce ar fi fost cele mai interesate de aceste informații.

David Sobei, consilier general în cadrul EPIC, s-a opus imediat conceptului ce a ajuns să echivaleze cu niște „identități guvernamentale” pentru oricine dorește să călătorească. Alte propuneri au ieșit la iveală curând, cum ar fi folosirea camerelor cu raze X și a profilurilor finanțate de stat. Sobell și alți activiști au protestat pentru simplul motiv că nicio bază de date atât de uriașă și de flexibilă precum CAPPSII nu poate fi precisă.

El a argumentat că FBI-ul a admis că baza sa de date privind infracțiunile are un procent de eroare de 33%. Cum sistemul CAPPSH a fost introdus fără ezitare, guvernul Statelor Unite a creat o listă cu persoanele care nu au dreptul să zboare și a început s-o aplice. Treptat, au apărut povești conform cărora tot mai multe persoane respectabile erau oprite la ghișeu, fiindu-le refuzată permisiunea de a se îmbarca. Au existat întotdeauna astfel de liste – atât în Marea Britanie, cât și în Statele Unite –, însă niciunul dintre indivizii ale căror nume erau transmise birourilor liniilor aeriene sau aeroporturilor din întreaga țară nu li se spunea de ce erau selecționate. Lista cu nume furnizată de comunitatea spionilor și de Departamentul Securității Interne părea să crească pe zi ce trecea. Deseori persoanele de pe ea aveau nume arabe sau

asiatice, dar rar existau explicații suplimentare. Orice tentativă de a pune sub semnul întrebării clasificarea celor care „nu li se permite să zboare” era imediat respinsă. Și specialiștii implicați în sistemul CAPPSII au devenit curând chiar ei îngrijorați cu privire la proiect proiectului, motiv pentru care acesta a fost trecut cu discreție pe linie moartă în perioada alegerilor prezidențiale din 2004. Apoi el a fost resuscitat. Simon Davies, reprezentant al grupului de presiune Privacy International, l-a descris ca „un dezastru gata să izbucnească”. El a spus: „Vor apărea erori judiciare și știm din experiențele anterioare că va fi un haos la o scară fără precedent în aeroporturile țării”.

Reprezintă oare CAPPSII viitorul? Singurul mod satisfăcător de a ne stabili adevăratele date de identitate este, în ultimă instanță, să avem un cip electronic implantat sub piele, cel mai sigur la naștere.

## Capitolul X

### Cum procedează europenii

*Odată cu Războiul din Irak, prăpastia politică dintre Europa și Statele Unite s-a adâncit considerabil. Francezii nu doar au refuzat să se implice în Războiul din Irak, ci au și câștigat un imens capital politic de pe urma poziției adoptate, iritându-i, în același timp, pe americani. În ciuda atacurilor cu bombă din 2004, de la căile ferate din Madrid, în Spania vecină, francezii nu par să se teamă prea mult de posibile violențe teroriste. Dacă vizitați Parisul sau Lyonul, o să observați că aceste orașe au și ele problemele lor legate de criminalitate și de imigrație, dar, cu toate acestea, supravegherea publică este cumva mai puțin intruzivă ca în Marea Britanie. Prin contrast, autoritățile britanice au dezvoltat o atitudine dezinhbată față de supraveghere, iar Marea Britanie a ajuns acum una dintre cele mai supravegheate țări din lume. Avem o lungă tradiție de activități teroriste în insulele britanice, iar orice semn care ar sugera o schimbare de comportament al IRA duce rapid la o creștere a supravegherii din partea statului și a activității serviciilor de informații.*

*Iar noi tindem să acceptăm această situație aproape fără să ne plângem, crezând, poate, că într-o zi problema terorismului va dispărea, iar lumea va reveni la normal.*

Dar cum stau vecinii noștri europeni? Ani de zile, olandezii au fost cei mai liberali oameni, totuși, toate acestea s-au schimbat când Pim Fortuyn a fost asasinat. Germania a suferit cât s-a aflat în mâinile grupului Bader Meinhof, dar țara a părut să aibă alte probleme în acea perioadă, iar terorismul



era ceva mai jos pe lista preocupărilor. Deci, ce se întâmplă cu Europa?

Odată cu Războiul din Irak, sentimentele antiamericane tot mai profunde ale francezilor au părut să întărească nevoia de libertate și intimitate a țării, în ciuda conservatorismului său inerent. Nu prea găsești supraveghere video în Franța și Germania, după ce ieși de pe autostradă. Punctele fierbinți ale criminalității din centrele orașelor sunt monitorizate câteodată, dar lucrul acesta nu este prea bine văzut și duce adesea la neliniști și demonstrații. De îndată ce camerele de supraveghere sunt instalate, membrii unui grup de presiune francez numit „Regardez Vous” („Priviți-vă”) apar, invariabil, și vopsesc cu negru lentilele camerelor. Gruparea a călătorit până și la New York și a demonstrat în Times Square. Violențele puse în practică la McDonald's, în Paris și în orașele și orașelele de provincie, nu se datorează doar unei percepții pe care o au unele grupuri franceze cum că acestea ar reprezenta niște simboluri culturale americane intruzive, ci și obiceiului acestei companii producătoare de hamburgeri de a instala camere pentru supravegherea clienților și, ocazional, a angajaților. Intransigența franceză referitoare la Războiul din Irak nu a făcut decât să înrăutățească lucrurile.

Americanii au decis să intre în forță în Irak în 2003, presupunând că și celelalte națiuni – și în special aliații lor tradiționali, precum Franța – vor fi bucuroase să cedeze puțin din autonomia lor națională, în schimbul prosperității și stabilității. America, în calitatea ei de cea mai puternică națiune a lumii, cerea de la celelalte state o recunoaștere clară a puterii sale și, de asemenea, un acord tacit cu viziunea Statelor Unite asupra situației politice globale de după sfârșitul Războiului Rece. Greșeala americanilor a fost să presupună că sprijinul automat va veni imediat după decizia de a intra în război împotriva Irakului.

Să alegi a fi aliat cu America era de bun-simț pentru mulți dintre politicienii de ambele părți ale divizatului eșichier politic din Marea Britanie. La urma urmei, puterea militară americană este fantastică, așa încât poate părea o idee bună să

beneficiezi de pe urma umbrelei sale protectoare. Și, oricum, pentru mult timp înțelegerea a sunat cam așa: „Ajutați-ne și o să vă ajutăm și noi”. Totuși, a existat un alt factor care a cântărit mai greu pentru europeni. Puterea Americii era atât de mare încât, atunci când a venit vorba de politica externă, Statele Unite aveau multe posibilități din care să aleagă, iar acest lucru o făcea să fie o țară imprevizibilă. Nu poți să știi niciodată în ce vei fi târât – și nici măcar dacă Statele Unite nu se vor întoarce într-o zi împotriva ta. Ce-și doreau Franța și Germania era o Americă mai previzibilă și rațională.

Statele Unite nu au realizat ca, timp de aproape un deceniu, acțiunile sale au fost percepute ca ostile în țări precum Franța, Germania, Rusia și China. Lumea islamică, în particular, a cam luat bătaie de la Statele Unite în Somalia, Bosnia, Kosovo și Irak. Intervențiile Statelor Unite, împotriva a ceea ce au fost considerate planuri ale Al Qaeda de creare a unui stat islamic transnațional, le-au permis, pur și simplu, grupurilor fundamentaliste musulmane să eticheteze America drept dușmanul islamului și să mobilizeze, astfel, un și mai mare sprijin pentru cauza lor. Al Qaeda s-a născut ca urmare a Operațiunii „Furtună în deșert” – invadarea Irakului în 1990, condusă de Statele Unite –, iar gruparea a prosperat de atunci încoace. Așa încât a existat opoziție la adresa războiului împotriva Irakului – și nu doar dinspre lumea islamică, ci chiar din partea vechilor aliați ai Americii din perioada Războiului Rece.

Francezilor, creșterea puterii americane li s-a părut o amenințare la adresa intereselor economice și strategice ale Franței în Orientul Mijlociu, așa încât readucerea Statelor Unite cu picioarele pe pământ a devenit parte a politicii externe franceze.

Franța era dedicată ideii unei Europe unite, care să acționeze pentru a contrabalansa Statele Unite, o Europă controlată împreună de Franța și Germania. Opoziția europeană față de America ar fi ajutat Comunitatea Europeană să crească, de la o simplă comunitate economică la o putere politică globală majoră. A existat un reziduu de

sentimente antiamericane în Franța încă de pe vremea Primului Război Mondial. Președintele francez Jacques Chirac credea, în 2003, că acest sentiment era împărtășit și de alte țări din Uniunea Europeană. Președintele Bush și-a făcut niște calcule greșite, așteptându-se ca Franța să ezite și să dezbată, pentru ca, în cele din urmă, să fie de acord să sprijine cauza și să spună „da” planurilor de detronare a lui Saddam Hussein și de instaurare a democrației în Irak. CIA a raportat că Franța era de acord cu credința britanicilor și americanilor, potrivit căreia Irakul avea arme de distrugere în masă și era pregătit să le folosească. Așa încât administrația Bush se aștepta ca Franța să fie de acord cu poziția Statelor Unite sau să fie forțată să ia poziție în fața Națiunilor Unite și să explice de ce țara era pregătită să tolereze armele de distrugere în masă din mâinile lui Saddam.

Statele Unite nu au reușit să înțeleagă faptul că Franța vedea decizia americană de invadare drept Șansa ideală de galvanizare a Europei sub conducere franceză. Statele Unite nu au înțeles nici gradul de preocupare a Franței privind creșterea puterii americane, care devenise amenințătoare pentru interesele europene și franceze în Orientul Mijlociu. Statele Unite mai credeau că au un aranjament cu Franța care ar fi apropiat cele două țări dacă și când Irakul ar fi refuzat să permită inspectorilor pe probleme de înarmare ai ONU să intre în țară, în noiembrie 2002. Cu toate acestea, președintele Chirac nu avea nicio intenție să fie de acord cu acest plan, și, pe fundalul sondajelor de opinie din întreaga Europă, care în proporție covârșitoare se împotriveau războiului, s-a străduit să creeze o coaliție antirăzboi.

În ianuarie, Franța, Germania și Rusia au respins, în cor, rezoluția ONU de autorizare a războiului împotriva Irakului.

Secretarul apărării din Statele Unite, Donald Rumsfeld, a ținut un discurs prin care a descris Franța și Germania drept „vechea Europă”. Suna ca o gafă tactică, dar, de fapt, declarația era menită să izoleze Germania și Franța de restul Europei, din pricina unei temeri în creștere față de o axă franco-germană care ar domina politica externă a Europei.

Spre sfârșitul secolului XX, Franța s-a lansat în construcția unui sistem de supraveghere prin satelit, ambițios și provocator, destinat să adune informații de spionaj. Din multe puncte de vedere, el este în linie cu Echelon, programul de supraveghere globală condus de Marea Britanie și America. Echelon se bazează pe o flotă de sateliți militari și stații de recepție de pe tot globul și s-a transformat în cel mai mare proiect mondial de colectare a informațiilor de spionaj. Acum însă există semne clare că, prin intermediul Franței și al sateliților săi Helios, țările europene au un sistem propriu de supraveghere internațională.

Franța are trei sateliți-spion pe orbită, toți operând în legătură cu o rețea de stații de recepție care, împreună, monitorizează, colectează și transmit sistematic informații către Statele Unite și alte țări. Se știe că au fost construite stații de monitorizare în Guyana Franceză, în orașul Domme din regiunea Dordogne (sud-vestul Franței), în Noua Caledonie din Pacificul de Sud și în Emiratele Arabe Unite. Stațiile franceze de monitorizare din Noua Caledonie și din Emiratele Arabe Unite sunt utilizate pentru a recepta transmisiunile de la sateliții din spațiu și pentru a acoperi transmisiunile din Asia și din Orientul Mijlociu. Posturile de receptare din Caraibe sunt folosite pentru a intercepta conversațiile din Statele Unite.

Nu este un sistem exclusiv militar și, așa cum se întâmplă și cu Echelon, datele obținute sunt trimise deopotrivă către piețele comerciale și militare. Proiectul francez este un prim pas către o încercare paneuropeană de a concura cu activitățile de spionaj globale ale Statelor Unite. Proiectul francez este operat de către Direcția Generală de Securitate Externă (DGSE), o agenție de supraveghere și spionaj organizată similar cu CIA. DGSE a intrat, de asemenea, într-un acord cu agenția germană de informații externe, Bundesnachrichtendienst (BND), pentru împărtășirea informațiilor extrase cu ajutorul programului Helios, în schimbul unei finanțări parțiale a proiectului. Informațiile comerciale sunt transmise direct către conducătorii

companiilor franceze și germane finanțatoare, dar și către serviciile secrete franceze. Existența unui sistem de supraveghere globală nu a fost niciodată confirmată sau negată oficial de către guvernul francez, deși existența lui este acceptată în general de către publicul francez și este cunoscută în comunitatea internațională a spionilor.

Spre deosebire de Echelon și de stația americană de receptare din Menwith Hill, a cărei existență este, de asemenea, cunoscută în Marea Britanie și Europa, nu prea există dovezi oficiale că Franța sau orice altă națiune europeană ar practica o supraveghere sistematică a comunicațiilor civile și militare internaționale. Acesta este unul din subiectele asupra cărora nu se comentează niciodată. Oficialii britanici care sunt familiarizați cu sistemul francez admit, în privat, că acesta există, dar spun că ar fi considerabil mai mic decât Echelon. Ziarul francez *Le Point*, într-un reportaj despre spionajul francez, a citat un oficial guvernamental care ar fi spus că, în vreme ce Echelon interceptează aproximativ 3 milioane de mesaje pe minut, sistemul francez interceptează vreo 2 milioane de mesaje pe lună. Dar adevărul este că nimeni nu știe nimic sigur, iar Direcția Generală de Securitate Externă (agenția însărcinată oficial cu securitatea externă, citată mai sus) face, în mod firesc, economie de știri. Ceea ce se știe este că francezii și-au actualizat unitățile de spionaj prin satelit de la data acelui raport și că vor continua să facă acest lucru.

Totuși, Franța măcar a recunoscut că dezvoltă un sistem de supraveghere internațională. François Rouselly, șeful personalului din cadrul Ministerului Apărării francez, a admis că sistemul, este utilizat pentru monitorizarea crizelor internaționale care prezintă interes militar pentru armata franceză, dar și pentru combaterea terorismului și prevenirea răspândirii armelor neconvenționale. Franța a strâns legăturile pe probleme de spionaj cu vecinii săi (Marea Britanie, Germania, Spania și Italia). Ar fi fost o nebunie să nu facă acest lucru. DGSE a fost în contact strâns cu MI5 în timpul procesului teroristului algerian Bourgass și are legături cu

unitățile din Poliția Metropolitană engleză care se ocupă de moravuri și de traficul de persoane. Franța este placa turnantă pentru infractorii care călătoresc dinspre Africa spre coastele vestice ale Europei și dinspre Balcani spre Europa. Adevărul este că Europa devine tot mai mult o unitate de spionaj și de colectare de informații, cu putere și resurse care rivalizează cu cele ale Statelor Unite.

Interceptarea de comunicații de către DGSE nu se află sub incidența legilor franceze legate de interceptări, care cere ca indivizii ale căror comunicații sunt înregistrate să fie suspecti de infracțiuni, după cum precizează Comisia Națională de Control al Interceptărilor de Securitate. Supravegherea franceză are, aproape sigur, obiective mult mai îndrăznețe. Înregistrarea comunicațiilor, așa cum este ea practică de DGSE, nu trebuie să fie neapărat legată de obiectivul de prevenire a activităților infracționale obișnuite.

Se crede că sistemul francez ar ținti spre sateliții de comunicații civile Intelsat și Inmarsat, printre altele. Sateliții folosiți în proiectul de supraveghere francez sunt din seria Helios, în interiorul unui program numit Euracom. Totuși, se pare că sateliții originali, lansați la sfârșitul anilor 1990, încep să-și arate vârsta și au o capacitate tehnică de interceptare și retransmisie comparativ scăzută. Drept urmare, se spune că francezii au pornit o inițiativă experimentală numită „Cerise”, pentru interceptarea comunicațiilor prin satelit. Ei au lansat recent un satelit militar de supraveghere Helios mai eficient, numit 2A. El a fost proiectat și construit în Franța, având o putere și o capacitate mult mai mari decât oricare dintre predecesorii săi.

Ultimul model Helios 2A a fost lansat pe orbită de către racheta europeană Ariane, în 2004. El este primul dintr-o nouă generație de sateliți-spion lansați de Franța. Cântărește peste 4 tone și a fost construit de consorțiul industrial condus de EADS-Astrium. Conform francezilor, 2A este destinat să marcheze începutul unei provocări europene la adresa dominației, din cadrul NATO, a serviciilor de informații ale Statelor Unite. Racheta Ariane-5 a decolat de la baza de

lansare, a Agenției Spațiale Europene (ESA) din Guyana Franceză, pe coasta de nord-est a Americii de Sud. La o oră după decolare, Helios 2A s-a separat de rachetă, apoi șase „microsateliți” au fost eliberați de rachetă în spațiu.

Ministrul apărării francez, Michèle Alliot-Marie, spunea: „În Europa, vorbim despre cele patru libertăți ale Uniunii – fluxul liber de informații, dreptul la liberă circulație, libertatea bunurilor și libertatea serviciilor –, dar mai există o a cincea libertate, care este informația de spionaj. Națiunile vor să-și aroge libertatea de a spiona”. Ea a făcut un apel la o mai mare cooperare europeană în ceea ce privește inițiativele de apărare spațială. „Cu Helios, forțele militare franceze pot beneficia de capacități sporite, de o capacitate de reacție mai precisă și mai rapidă. Statutul de putere în spațiu a devenit esențial, dacă vrei să exiști pe scena mondială”. Sateliții Helios I, dintr-o generație mai veche, lansați în spațiu de către rachetele Ariane în 1995 și 1999, erau, tehnic, mai puțin sofisticati – și urmează să fie înlocuiți. Locotenent-colonelul Inaky García Brotons, din Forțele Aeriene Franceze, a declarat agenției de știri Reuters, înainte de lansare: „Acest satelit este indiscutabil mai sofisticat. Sistemul cu infraroșii ne oferă o detectare mai precisă a activităților umane. De exemplu, pe vizibilitate redusă sau noaptea, ne poate spune dacă un convoi de camioane se mișcă sau staționează, sau dacă un reactor nuclear este operațional sau nu”.

Oficiali din domeniul apărării din Franța spuneau că, deși generația Helios 2 poate să opereze noaptea, nu poate, totuși, prelua imagini prin nori groși. Costul total al programului, care include un al doilea satelit ce va fi lansat în următorii trei ani, a fost de peste două miliarde de euro (2,6 miliarde de dolari), din care Franța acoperise 95%. Francezii sunt remarcabil de reticenți în ceea ce privește flota lor de sateliți de supraveghere și planurile lor de a investi și mai mult în echipamente de supraveghere militară din spațiu. În ciuda unui cor tot mai puternic de dezaprobare din partea grupurilor franceze de apărare a drepturilor cetățenești, nu par să existe informații credibile privitoare la regularitatea

posibilelor interceptări, a ȋntelor specifice sau a volumului traficului.

Conform unei dări de seamă apărute în de *Journal Officiel de la République Française*, ziarul care publică zilnic activitățile legislative guvernamentale, există niște acorduri între agențiile de spionaj franceze și germane de împărțire a costurilor supravegherii globale prin satelit. Într-o interpelare adresată biroului premierului, privind operațiunile de spionaj, Nicolas About, un deputat francez, făcea o declarație înfiorătoare: „Salutăm resursele pe care guvernul le-a investit în legea acoperind operațiuni militare de recrutare în serviciile de securitate și pentru abilitățile operaționale dovedite în cadrul programului franco-german de supraveghere prin satelit”. Această declarație pare să confirme faptul că cele două guverne cooperează, în prezent, în chestiunea sateliților militari, care pot să spioneze atât populația Franței, cât și extremiștii islamici din Algeria. Sateliții Helios sunt folosiți în misiuni de recunoaștere fotografice, iar datele obținute din supraveghere sunt împărțite agențiilor de informații din Germania, Spania și Italia.

Există constrângeri financiare evidente pentru acest tip de tehnologie, dar acesta nu este singurul motiv pentru a investi în acest tip de program și a-l extinde, implicându-i pe aliații europeni. Implicarea financiară germană în acest sistem ne ajută să înțelegem de ce administrația Bush nu a reușit, în ciuda unor eforturi susținute, să convingă Bonnul să respingă sateliții militari francezi și să accepte ajutorul Statelor Unite pentru a construi capacități germane de adunare de informații. Francezii au investit recent în patru sisteme AWACS E-3 (Sisteme de Avertizare și Control Aeropurtate). Sistemul AWACS a fost selectat ca fiind cel care îndeplinește cerințele inițiale referitoare la avertizările aeropurtate ale Republicii Franceze. Această navă reprezintă standardul mondial pentru sistemele de avertizare aeropurtată timpurie; E-3 a fost proiectat și livrat de către Boeing, iar cele patru E-3-uri ale Forțelor Aeriene Franceze îndeplinesc atât funcții de



supraveghere aeriană, cât și funcții de comandă și control. Le-au fost adăugate funcții de îmbunătățire a supravegherii, pentru a îndeplini standardele franceze unice pentru misiuni și au o capacitate foarte mare de interceptare și transmitere a semnalelor de la sol sau de la sateliți. Ele folosesc un sistem de realimentare prin sondă, pentru a crește receptaculul existent de alimentare în timpul zborului, un înregistrator digital pentru misiunile audio și echipamente radio îmbunătățite. Conform unei surse RAF, sistemul francez ESM de avertizare timpurie și de supraveghere AWACS este un sistem pasiv de ascultare și de detecție care permite lui AWACS să detecteze, identifice și urmărească electronic transmisiile unor surse de la sol, din aer sau maritime. Folosind sistemul ESM, operatorii misiunilor pot identifica tipul radarului sau al armelor. Un element major de sprijin direct îl reprezintă instalația franceză a echipamentului misiunii E-3. Boeing a livrat o navă goală pe aeroportul Le Bourget, de lângă Paris, acolo unde au fost instalate sistemele franceze.

Un fapt inevitabil este acela că, în Europa și în Statele Unite, atât guvernul, cât și industria sunt de acord că „spionajul prietenos”, din rațiuni politice și economice, este răspândit printre aliații occidentali. Cu alte cuvinte, supravegherea, spionajul industrial, furtul de secrete și trasul cu urechea, deși nu sunt acceptabile într-o societate civilizată, sunt folosite oricum. Raportul anual al STOA (Evaluarea Opțiunilor Științifice și Tehnologice), organism al Parlamentului European, detaliază operațiunile de supraveghere ale Statelor Unite; cu toate acestea, Statele Unite au fost scandalizate la gândul că spațiul le este invadat, iar rețelele de comunicare le sunt spionate. Statele Unite acuză națiunile europene, precum și alte țări, de „spionaj și colectare globală de informații”, incluzând și operațiuni de ascultare a cetățenilor și a companiilor americane.

Centrul Național pentru Contrainteligență (NACIC) al Statelor Unite, afirmă, în raportul său anual, că „guvernele străine care conduc activități de spionaj industrial” reprezintă

o preocupare reală și majoră și, cu toate acestea, nu a fost nominalizată nicio țară anume. „O serie de țări străine ridică amenințări la diferite niveluri și de diferite tipuri, pentru informațiile economice și tehnologice ale Statelor Unite. Majoritatea acestor țări sunt fie aliați pe termen lung ai Statelor Unite, fie țări neutre în mod tradițional. Ele au început să țină seama și să captureze informații economice și tehnologice din Statele Unite, în ciuda relației lor prietenoase cu Statele Unite”.

Franța este, fără îndoială, una din cele mai active țări din lume în direcția adunării de informații – și se consideră a fi în fruntea Europei, când vine vorba de demonstrarea puterii europene. Furtul de informații industriale și economice nu este, de obicei, așa de sofisticat precum mulți dintre noi s-ar aștepta și există o largă paletă de posibilități pentru cei implicați în adunarea de informații care i-ar aduce avantaje în afaceri. De exemplu, domeniul telecomunicațiilor este ținut și interceptat în mod direct. Cea mai lucrativă dintre toate posibilitățile, neglijența referitoare la codarea secretă (criptare) a datelor din sectorul privat, lucru care face posibilă obținerea lejeră de mari cantități de date. Francezii admit că aceste tehnici le oferă cea mai mare parte din informațiile economice și industriale obținute de la corporațiile americane.

Firmele de telecomunicații deținute de stat reprezintă o altă țintă pentru supravegherea și spionajul de stat, iar transmisiile de date vrac din computere și din poșta electronică și traficul de faxuri reprezintă o țintă prioritară, deoarece sunt ușor de accesat și interceptat. Telecomunicațiile corporatiste și în special telecomunicațiile internaționale reprezintă, de asemenea, o sursă de informații, foarte vulnerabilă și eficientă, potrivit unor surse neoficiale din cadrul NACIC.

Comunitatea agențiilor de informații ale Statelor Unite acuză deseori națiunile străine care practică spionajul economic în detrimentul firmelor din Statele Unite. FBI-ul nominalizează Franța, Germania, Israelul, China, Rusia și Coreea de Sud în mod constant printre culpabili. Această dezvăluire, evidentă și, în general, lipsită de necesitate, a

Biroului, a fost făcută de Edwin Fraumann, un agent FBI de la sediul din New York, care a redactat o analiză academică asupra spionajului comercial internațional, publicată de Societatea Americană a Administrației Publice, în *Public Administration Review*. Fraumann a pretins că agenții francezi îi interceptau până și pe oamenii de afaceri americani care zburau cu avioanele companiei naționale Air France, precum și convorbirile telefonice și comunicațiile prin fax din hotelurile franceze. Analiza continua și acuza Germania că operează un post de supraveghere în apropiere de Frankfurt, de unde se monitorizează convorbirile telefonice din Statele Unite și că încearcă să penetreze sistemele de computere americane. Comparativ cu Echelon, bineînțeles, asta nu e mare lucru. Dar nu prea există îndoială: aceste înregistrări și monitorizări ale unui grup select de vizitatori, în special din America, sunt constante și profesionale.

Și cu siguranță că nu există nicio îndoială că Echelon colectează cantități imense de date confidențiale despre afacerile europene. Indignarea Americii este, în consecință, deplasată și exprimată doar ca parte a unui proces de propagandă. Bernd Schmidbauer, directorul serviciilor secrete germane, a negat acuzațiile într-un articol și a declarat că spionajul străin împotriva firmelor germane reprezintă o problemă serioasă și costisitoare. Ca reacție, Franța și Parlamentul European au criticat operațiunile globale de supraveghere ale Statelor Unite și s-au arătat reticente în a coopera în operațiuni de spionaj transfrontalier cu America, din cauza riscului de a atrage o limitare a dreptului la viață privată a cetățenilor și de a încuraja spionajul împotriva companiilor europene. Oficiali ai guvernului francez au confirmat că țara a decis să-și schimbe politica de criptografie în ianuarie 1999, iar acum încurajează utilizarea criptării, din cauza gradului de sofisticare a capacităților de interceptare ale Statelor Unite. Ministrul afacerilor externe francez, Hubert Vedrine, spunea în noiembrie 1998 că, pentru guvernul francez, a devenit o „preocupare” contrabalansarea amenințării reprezentate de Echelon. De fapt, atât Franța, cât

și Statele Unite s-au suspectat una pe cealaltă în probleme de spionaj, iar o escaladare a acestei situații datează din perioada Războiului Rece, când Franța a creat politica de reconciliere cu URSS-ul, numită „A Treia Cale”. La începutul anilor 1990, Franța a respins inițiativa FBI-ului de cooperare pentru crearea unei baze de date internaționale referitoare la teroriști, pur și simplu pentru că programul era condus de Statele Unite.

„Spionajul prietenos” este un eufemism pentru comportamente de natură să ridice temperatura relațiilor diplomatice. Au fost raportate multe incidente de spionaj comercial și diplomatic între țările occidentale prietene, lucru care a dus la tensiuni între Europa și Statele Unite. În decembrie 1995, cinci angajați ai Ambasadei Statelor Unite au fost expulzați din Franța după ce au fost acuzați a fi agenți CIA. A fost un incident public straniu, cu implicații politice profunde, care a survenit în timpul campaniei electorale pentru prezidențialele din Franța și care l-a făcut pe un agent de informații din Statele Unite să declare (către *The Washington Post*) că va dăuna cooperării americano-franceze pe probleme de spionaj pentru mulți ani de-atunci încolo. Nu fusese nimic altceva decât un gest politic tipic francez destinat să adune voturi. Dar americanii nu au uitat niciodată. Ca o altă ripostă la criticile SUA la adresa Europei, un cetățean american a fost deportat din Germania, în martie 1997, pentru încercarea de mituire a unui oficial din Ministerul Economiei.

Cooperarea cu Statele Unite, în Europa, nu este neapărat o politică bună, din cauza tensiunilor interne create inevitabil de către acuzațiile lansate de inițiativele americano-europene de supraveghere reunită. Mulți membri ai Parlamentului European și oficiali ai Comisiei Europene sunt reticenți când e vorba să accepte orice tip de acord de cooperare pentru activitățile de interceptare ale polițiilor europene. Motivul este acela că mulți politicieni europeni văd asta drept încă o cale de întărire a relațiilor cu FBI-ul și cu CIA-ul. S-a afirmat că „Rezoluția asupra Interceptării Telecomunicațiilor în Contextul Noilor Tehnologii” a Consiliului de Miniștri al UE ar

fi fost schițată cu ajutorul FBI-ului, iar grupul de luptă pentru drepturi cetățenești Statewatch, cu sediul în Marea Britanie, prezenta un document care părea a fi un document de lucru confidențial al Consiliului, care afirma că FBI-ul participase la schițarea rezoluției în calitate de „grup de experți” pentru cerințele tehnice ale interceptării.

Nimeni nu pare pregătit să confirme faptul că Rezoluția Consiliului pe Probleme de Interceptare Polițienească (ENFOPOL 98) a avut ca scop doar aplicarea legii sau s-a dorit ca ea să abiliteze o interceptare globală a comunicațiilor. În Europa s-au făcut apeluri la cooperarea serviciilor secrete din interiorul Comunității Europene, și, mai exact, într-un document de lucru al Uniunii Europene Occidentale, alianța militară a Europei, intitulat „O politică europeană a serviciilor secrete”. Un astfel de program ar presupune o colectare de informații din zone aflate în afara celor privite de obicei ca preocupări tradiționale legate de securitatea națională. Este evident că, dacă UE prosperă și se consacră ca o putere militară mondială, atunci trebuie să aibă și capacitatea de a sprijini acest lucru prin activitățile serviciilor de informații. Aceste activități s-au schimbat serios în ultimii ani. Au fost dintotdeauna o chestiune militară, care depindea, într-o mare măsură, de spionajul uman („Humint”) drept sursă. Deși sunt încă de uz militar, activitățile serviciilor moderne de informații au aproape întotdeauna și o latură politică, comercială sau religioasă.

Toate guvernele europene sunt cu ochii pe unitățile de supraveghere ale Statelor Unite, stare de spirit care face, în mod firesc, ca orice cooperare transatlantică în domeniul informațiilor să fie dificil de realizat. În vreme ce Marea Britanie a cooperat total cu Statele Unite în timpul Războiului din Irak și după acesta, supravegherea a devenit, în Europa, o chestiune pur europeană – și continuă să fie astfel. Unitatea politică și economică întărită prin crearea unei monede unice ar putea fi extinsă și spre alte zone, cum ar fi o abordare europeană conjugată a tehnologiilor de supraveghere, pe care Franța încearcă, fără îndoială, să o conducă.

Drept urmare, în locul creării unui sistem unic de supraveghere globală a Europei și Statelor Unite, dacă Franța și Germania își vor face voia, Europa va ajunge în cele din urmă să-și realizeze propriul proiect independent, care să-l concureze pe cel al Statelor Unite. O rețea paneuropeană independentă, de spionare și supraveghere, nu îi va face pe adeptii dreptului la viață intimă să doarmă mai liniștiți în paturile lor, la gândul că drepturile cetățenești le sunt protejate. Ce se va întâmpla însă va fi că lumea se va trezi cu două sisteme puternice și intruzive de supraveghere, în loc de unul.

Este evident că Franța are acum resursele tehnologice necesare pentru supravegherea globală și că le folosește. Iar aceasta ar putea servi drept început pentru o inițiativă europeană de colectare a informațiilor, ceea ce va însemna, probabil, că adunarea de informații există și în afara unor legi naționale consacrate, destinate să protejeze viața privată. Și în arena politică, și în cea comercială, Europa și-a întărit securitatea informațională, prin intermediul tehnologiilor de criptare și de monitorizare electronică, pentru a se proteja de posibilele interceptări ale comunicațiilor din partea Statelor Unite. Motivația Europei de a investi în tehnologie de supraveghere și de a dezvolta astfel de tehnologii este, evident, aceea de a contrabalansa cunoștințele tehnologice ale Statelor Unite. O dificultate majoră este aceea că Statele Unite, în lupta împotriva amenințării globale a terorismului, solicită acces imediat la informațiile referitoare la teroriști. Nu este în interesul nici unei țări să refuze accesul la aceste informații, ceea ce înseamnă că relațiile între Statele Unite și fiecare țară din Europa\* la nivel operațional, trebuie să continue să existe. De exemplu, după atacul cu bombă de la Madrid, din martie 2004, noi dovezi ale modului în care teroriștii islamiști au reușit să nu fie detectați, prin aceea că au operat în rețele slab conectate, au apărut ca urmare a unei investigații realizate de agenții de spionaj din Paris și Madrid. La 11 zile după atrocitățile din capitala Spaniei, descoperirea legăturilor politice dintre un suspect principal în atacul cu

bombă și militanții islamiști de peste tot din Europa și din Africa de Nord a făcut dovada creșterii numărului de rețele teroriste cu puține legături directe cu Al Qaeda, dar cu intenții similare. Atacul a dezvăluit o „acumulare de straturi din diferite rețele care fuseseră slăbite, dar care au reușit să fuzioneze și să se regenereze”, după cum spunea Jean-Charles

Brisard, fost agent al unui serviciu secret francez, care a investigat Al Qaeda pentru avocații care au reprezentat familiile victimelor din 11 septembrie.

„Regenerarea unor grupări teroriste ilustrează modul în care amenințarea terorismului s-a mutat dinspre Al Qaeda spre niște organizații asociate, inspirate de Bin Laden, dar care, nu așteaptă neapărat ordine de la acesta”, spunea doctorul Rohan Gunaratna, care a scris cartea *în interiorul Al Qaeda: Rețeaua globală a terorii.*, Acest lucru arată că Al Qaeda a devenit o mișcare și nu mai este un singur grup”. De câte ori se întâmplă o atrocitate, oriunde în lume, Statele Unite află mai multe despre inamicul pe care și-a propus să-l urmărească fără remușcări. Cheia, spune doctorul Gunaratna, este o cooperare internațională strânsă a serviciilor de informații. „Serviciile de securitate europene încă mai privesc rețelele de teroriști ca pe niște probleme naționale”, afirmă el. „Ele nu au ajuns la nivelul de integrare pe care l-a atins Al Qaeda, în ceea ce privește combinarea rețelelor”. Totuși, Statele Unite l-au atins.

Desigur, există grupuri de apărare a drepturilor cetățenești care văd pretutindeni conspirații hotărâte să ne deposeze de dreptul la intimitate, mai ales când vine vorba de cooperarea dintre comunitatea de spionaj americană și Europa. E de înțeles de ce asta face pe toată lumea nervoasă. Drepturile cetățenești reprezintă foarte mult în Paris și Bonn, iar Parlamentul European vede cu ochi răi incursiunile în Europa ale unor agenții de spionaj externe, precum FBI și CIA. Cererile frecvente și mereu respinse venite de la Bruxelles despre ce se întâmplă la Menwith Hill nu sunt de folos. E de înțeles faptul că Franța și Germania doresc să aibă propriile capacități în această zonă.

Distanțarea de Statele Unite în probleme de spionaj vine împreună cu o tendință către cooperare interguvernamentală în domeniul impunerii legii, manifestată de exemplu prin eforturile celor mai bogate țări din lume (Grupul celor Opt și Grupul de la Lyon) de a combate infracțiunile high-tech sau prin acordul de la Wassenaar privind controlul exportului de tehnologie pentru criptare.

În timp ce aceste discuții internaționale continuă, activitățile de supraveghere orientate împotriva cetățenilor și companiilor unor națiuni aliate, cu scopuri diferite de tradiționala securitate națională, continuă și ele. Guvernul german a aprobat o lege de spionaj menită a înlesni autorităților posibilitatea de a trage cu urechea la comunicațiile prin telefoane fixe sau mobile, e-mail, fax și SMS (serviciul de mesaje scurte). Noua lege le cere furnizorilor de rețele să instaleze și să mențină echipament și proceduri care oferă acces la traficul electronic al clienților lor, odată ce autoritățile au obținut un ordin legal de supraveghere. Trasul cu urechea „în cazul suspiciunii de anumite infracțiuni grave” este, se pare, deja permis în legislația existentă.

Legea nu se aplică în cazul companiilor private de telefonie, iar cerințele tehnice sunt limitate la furnizorii de „sisteme de telecomunicații publice”, care includ operatori de telefonie la sol și mobilă sau furnizori de conturi e-mail, dar nu și furnizori de servicii internet. Operatorilor unor modalități de transmisie care oferă utilizatorilor acces imediat la internet, cum sunt conexiunile DSL (linie de abonament digital), li se cere de asemenea să-și instaleze tehnologia de interceptare. În Germania, cel mai mare astfel de operator este Deutsche Telekom AG, fostul furnizor obligatoriu de telefonie, care este încă deținut majoritar de stat. Guvernul german afirmă că propuneri privind interceptarea convorbirilor au existat dinainte de 9/11, dar au fost aspru criticate de industriile IT și de telecomunicații, care s-au plâns cu privire la costurile mari ale instalării tehnologiei necesare. Desigur, 11 septembrie a schimbat situația și industria a acceptat, în



cele din urmă, o soluție de compromis.

Normal, nu toate temerile industriale au fost satisfăcute de noua lege, potrivit asociației profesionale IT BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien eV), dar legislația în vigoare oferă aparent un compromis acceptabil între interesele statului de supraveghere a telecomunicațiilor și utilizarea neîngrădită a internetului. Planul original ar fi implicat supravegherea angro a furnizorilor de servicii, însă compromisul acceptat de guvernul german pune accentul pe conexiunile utilizator-rețea, ceea ce, afirmă industria, face viața mai ușoară pentru furnizorii de rețele mai mici și de servicii internet.

Bineînțeles, organizațiile de drepturi cetățenești nu au fost potolite prea ușor. 12 grupuri de apărători ai drepturilor omului au compus o declarație comună, avertizând asupra pericolului unui „stat supraveghetor” și menționând experiențele totalitariste ale țării, precum nazismul și comunismul est-german. „Balanța dintre libertățile cetățenești garantate de lege și dreptul statului de a le încălca nu trebuie să fie abolită în interesul unei securități naționale abstracte”. Grupurile, care sunt puternice și luate în serios în Germania, includ Uniunea Umanistă, Asociația Germană pentru Protecția Datelor și grupul hackerilor, Clubul de Haos al Computerelor. Ele afirmă că se împotrivesc nu doar legii privind interceptarea telecomunicațiilor, ci și altor măsuri de securitate propuse, cum sunt luarea amprentelor, oferirea datelor studenților către poliție sau supravegherea crescândă a străinilor.

Poate fi argumentat că germanii doar aduc protecția cetățenilor lor la același nivel cu celelalte țări. Statele Unite și Marea Britanie permit interceptarea, iar în Franța au fost promulgate legi ce permit „decriptarea, în anumite circumstanțe, a mesajelor criptate transmise prin intermediul internetului”. Grupurile de apărare a libertăților cetățenești au replicat: „Aproape toate măsurile propuse se opun unor drepturi de bază. Însă niciuna nu oferă mai multă siguranță cetățenilor”. Un purtător de cuvânt al guvernului german a

spus: „Dacă nu aveți nimic de ascuns, atunci nu aveți de ce să vă faceți griji”. Oare unde am mai auzit asta?

## Capitolul XI

### Nu votați pentru asta

*Alegerile generale britanice din 2005 au fost o afacere deosebit de nesatisfăcătoare. Dezbaterile păreau limitate și banale, fără nicio consistență reală. Mass-media părea să se concentreze asupra promisiunilor încălcate și a imoralității campaniei de management. Și totuși, a fost desfătarea supremă pentru un om de marketing! Au fost cheltuite sume enorme în cinci sau șase săptămâni de activitate frenetică. Ambele partide importante au avut echipe mari de campanie, pe care presa\* cu obsesia ei pentru cultura celebrității, s-a străduit să le transforme în subiecte de ziar.*

Cea mai mare parte din acțiune s-a desfășurat în circumscripțiile marginale, unde câțiva alegători „indecisi” dețineau cheia rezultatului general. Majoritatea acestor locuri aparțineau Noilor Laburiști. La începutul campaniei electorale, toate partidele politice importante credeau că lupta va fi câștigată sau pierdută în aceste secții marginale vitale. Managerii alegerilor, care au fost nevoiți să-și înghesuie planurile într-un interval de câteva săptămâni, au fost apoi obligați să-i identifice pe alegătorii pe care voiau să-i abordeze și să-și concentreze mesajele asupra lor cât mai convingător posibil. Cea mai eficientă metodă pentru a reuși era prin intermediul publicității și al poștei directe. Aveau mijloacele pentru a-i aborda pe alegători prin telefon, poștă sau contactându-i personal. Dar cum te pui de acord asupra mesajului pe care vrei să-l transmiți? Intenția mesajelor politice este să se adreseze în același timp persoanelor individuale, familiilor, comunităților. Ele răspund preocupărilor legate de mediu, impozitare, imigrare etc. Dar cum pot descoperi echipele de campanie electorală ale unui

partid ce anume îl motivează pe un alegător dacă nu știu absolut totul despre el sau ea? Problema lor cea mai evidentă, ai putea crede, e că nimeni nu poate ști atât de mult despre un individ. De fapt, nu e chiar adevărat. Cu puțin timp la dispoziție și acces la câteva dosare personale, un analist experimentat poate pune cap la cap destul de ușor ce-l motivează pe un individ. Se întâmplă tot timpul.

Alegerile generale din Marea Britanie din 2005 vor rămâne în amintire mai degrabă pentru ceea ce nu s-a discutat decât pentru ceea ce s-a spus. Europa, de exemplu, a fost un subiect uitat; n-a fost menționat aproape niciodată, și totuși viitorul Marii Britanii în Europa, după cum a dovedit-o referendumul pentru noua Constituție europeană, va fi una dintre cele mai importante probleme politice ale vremurilor moderne. Nimeni din Partidul Conservator n-a sărit la bătaie pentru economie sau cheltuielile de apărare, sau regiunile rurale. Se prea poate ca aceste subiecte să fi apărut ca probleme locale, dar la nivel național se pare că s-au delimitat cu grijă câmpurile de bătaie de-a lungul unor linii înguste. A fost o campanie enervantă la culme din multe puncte de vedere. Au apărut discursuri în limbaj de ziar de scandal, iar sloganurile au fost scrise de PR-iști cinici și experți în trasul sforilor, și apoi repetate la infinit. Presa a stors tot ce-a putut despre conflict, analizând, studiind, condamnând și, în general, epuizând toate posibilitățile. Dar până și presa a părut să ezite când a venit vorba de alte probleme importante în afară de imigrare, foste dosare, gafe verbale sau voturi. Comentatorii politici, evident disperați să găsească ceva nou de spus, au căzut tot mai mult în extreme. În ajunul alegerilor, *Times*, pe vremuri o publicație londoneză respectabilă, a publicat o pagină pe care principalele două titluri spuneau: „Howard îndemnat să rămână și dacă este înfrânt” și „Sprijinul conservatorilor atinge cel mai mic nivel”.

Cunoașterea în detaliu a trecutului unui politician este de o importanță esențială în timpul alegerilor. Jurnalismul ziarelor de scandal trebuie să fie personal. Ca reporter, trebuie să aplice următorul test unei povești: răspunde la întrebările

„cine, ce, când, unde și de ce?” Elementul vital este întotdeauna „cine?”. Dosarele din baza de date Murdoch Press și Associated Newspapers conțin informații despre viețile și micile păcate ale celebrităților din lumea politică, industrială, show-business sau, pur și simplu, a celebrităților „înnăscute”. Dar marfa importantă e păstrată în biroul și seiful redactorului executiv. Când a fost redecorat biroul lui Paul Dacre și a rămas neîncuiat, angajații de la *Daily Mail* s-au servit din belșug din secretele lui și le-au vândut revistei satirice *Private Eye*, unde se mai păstrează încă o selecție savuroasă. În oarecare măsură, mass-media există ca să afle, să publice și să comenteze secretele și, la fel ca serviciile secrete, își va croi drum cu microfoane și intrări prin efracție oriunde în lume ca să obțină ceea ce-și dorește. Bărbații și femeile ale căror nume apar atât de des trebuie să aștepte ca să afle ce se va mai dezvălui despre ele în continuare – și când. Desigur, dacă și-au vândut poveștile prin intermediul unui agent, vor ști exact ce și când se va publica. Chiar și atunci, ziare rivale vor face dezvăluiri în avanpremieră. Acestea sunt povești pe care reporterii lor au reușit să le încropească din crâmpie de informații și jumătăți de adevăr pe care au reușit să le culeagă în legătură cu subiectul și cu evenimentul „senzațional” în chestiune. Intenția publicării detaliilor în avanpremieră este minimalizarea impactului „dezvăluirilor. În exclusivitate” ale celorlalte ziare, pentru a-și proteja vânzările. E greu să controlezi o poveste odată ce are „picioare”.

Când, în timpul campaniei electorale din 2005, l-am întrebat pe redactorul de știri de la un ziar național de duminică ce-și dorește cel mai mult pe lume, mi-a spus, fără ezitare, că vrea *fotografii cu Sandra Howard goală*. Se referea, normal, la pozele nude făcute în anii 1960, când Sandra Paul, cum se numea atunci, a avut o carieră de succes ca manechin. Se pare că toate manechinele din anii 1960 s-au dezbrăcat în fața camerei mai devreme sau mai târziu, de obicei pentru David Bailey. În ceea ce-l privește pe redactorul de la ziarul de duminică, cineva, undeva, deținea astfel de poze cu Sandra, iar el le voia. L-am întrebat, în cazul în care existau și reușea

să le cumpere, dacă le-ar publica în timpul alegerilor. A ezitat și apoi mi-a răspuns: „Doar să le am ar fi probabil de-ajuns”. Evident, nu avea nicio legătură cu conceptul de „știre”.

Dintre toate serviciile care strâng informații, presa este probabil cea mai lipsită de remușcări. Știe lucruri murdare despre toți cei din lumea politică – și politicienii o știu. În Fleet Street funcționează o rețea complicată de afaceri și înțelegeri nescrise. Unele aranjamente sunt bine cunoscute, precum cel dintre prințul de Wales și familia lui și haitele de paparazzi și urmăritori care nu-i dau pace niciodată. Înțelegerea este ca familia regală să permită „acces limitat în schimbul intimității”. Înțelegerea e încălcată adesea din cauza competiției disperate din haita de ogari ai știrilor, dar în general funcționează.

Dacă pornim de la premisa că redactori puternici ca Paul Dacre știu mult mai mult decât sunt dispuse ziarele să dezvăluie, trebuie să ne întrebăm care sunt implicațiile acestui lucru. De exemplu, Dacre și angajații lui ar putea ști că Lordul „A”, ministru, își înșală soția, dar preferă să n-o dezvăluie în ziar, iar Lordul „A” știe că Dacre e la curent, dar nu știe de ce el păstrează tăcerea. Oare faptul că Dacre are cunoștință de acest lucru pune în mod automat presiune asupra Lordului „A”? Oare simplul fapt de a deține această informație constituie o problemă serioasă? Cine ia decizia finală să publice o poveste? Și, poate chiar mai important, cum ajunge el sau ea să ia această decizie? În fiecare săptămână, mii de știri și articole sunt „aruncate” – refuzate la publicare. De obicei asta se întâmplă pentru că simt pur și simplu plictisitoare sau nefondate, sau calomnioase. Dar ce se întâmplă cu ceea ce nu se publică, dar se păstrează la dosar? Cine ia decizia să omoare o poveste înainte ca ea să fie lansată?

Acum câțiva ani, înainte de invazia în Irak din 2001, am petrecut aproape o săptămână într-o bază aeriană NATO din Insurlik, Turcia. Era la mijlocul lui decembrie, în cele șase luni dinaintea campaniei electorale, iar aerodromul era aproape de granița dintre Turcia și Kurdistan. Era un loc dezolant și

mizer, departe de zona turistică de pe coasta mediteraneeană, și era foarte frig. Insurlik, un oraș aflat la aproximativ 16 kilometri de bază, era zonă interzisă pentru piloți și pentru personalul de la sol al bazei militare. În parte, era din cauza rău-famatei închisori a datornicilor. Pe vremea aceea, dacă datorai bani în Turcia, stăteai la închisoare până-ți plăteai datoria. Dacă nu aveai niciun fel de bunuri sau bani, atunci singura ta opțiune era să-ți pui familia să se prostitueze. Rezultatul era că orașul devenise un loc periculos și violent, în special noaptea, iar comandanții taberei au interzis orice fel de contact cu populația autohtonă.

Baza propriu-zisă nu era un loc cu mult mai sigur. Turcii și kurzii erau în conflict, grupările teroriste kurde, cum e KSA, bombardau și împușcau populația civilă din Istanbul. Deși Insurlik era o unitate NATO unde se aflau detașamente de infanterie și flotilă aeriană turcești, americane, britanice și franceze, baza era în mod evident deținută de turci, și în săptămâna dinaintea sosirii mele aceștia instituiseră o oră de stingere pentru tot personalul militar care nu era turc. Patru zile mai târziu, o santinelă turcească a împușcat și ucis un soldat american care ieșise să facă jogging la asfințit, pe pista din perimetrul bazei.

În comparație cu americanii, care dormeau în barăci bine construite și puteau mânca la McDonald's sau puteau face cumpărături la PX, unde se vindea orice la prețuri de nimic, soldații RAF erau în mare măsură rudele sărace ale bazei. Popotele lor erau barăci de lemn și, în ciuda frigului extrem, erau forțați să doarmă în corturi. În fiecare zi, aparate de zbor Tornado britanice, F16 americane și turcești și Mirage franțuzești părăseau baza în număr mare, pentru a patrula spațiul aerian deasupra părții de nord a Irakului și pentru a institui zona interzisă de zbor, impusă de Națiunile Unite. Era o sarcină riscantă și delicată, iar radarele irakiene urmăreau adesea avioanele NATO pentru a le testa răspunsul.

După ce am petrecut trei sau patru zile în bază, am început să înțeleg că era ceva în neregulă. Relațiile cu comandantul turc erau „nesatisfăcătoare” în cel mai fericit caz, și câteodată,

fără nicio avertizare, acesta oprea zborurile de la bază, cu excepția activităților flotei turcești. Turcii erau bine antrenați și utilizați cu echipamente militare. Avioanele lor F16 americane erau cele mai bune aparate de zbor de atac din lume și dispuneau de toate resursele necesare, inclusiv bombe ghidate cu laser și rachete Hellfire aer-sol.

Echipajul aerian RAF era foarte nemulțumit, dar nu din cauza condițiilor în care erau nevoiți soldații să trăiască, nici a echipamentului cu care trebuiau să lucreze. Cu două zile înainte de data când trebuia să iau avionul Hercules înapoi spre Londra, am descoperit că ceea ce nemulțumea echipajul aerian era ceea ce se întâmpla când turcii limitau zborurile numai la aparatele de zbor turcești. Un important ofițer de zbor RAF mi-a spus că turcii începuseră de curând misiuni de zbor la nivel jos în munții din sudul și estul orașului Mosul, de unde bombardau cu napalm satele kurde.

Faptul că avioane NATO, purtând însemnele NATO, bombardau cu napalm așezări civile era normal să-i deranjeze pe soldații britanici, și baza era cuprinsă de mânie și neliniște. Aveau înregistrarea de supraveghere aeriană cu efectele bombardamentului, iar unii pretindeau chiar că le văzuseră în timpul patrulelor menite să-l limiteze pe Saddam Hussein la bazele lui aeriene și să monitorizeze mișcările militare din partea de nord a Irakului. M-am întors la timp la Brize Norton la sfârșitul săptămânii și mi-am trimis reportajul și fotografiile la *Mail on Sunday*. Asta se întâmpla în vremurile nu prea îndepărtate când poșta electronică era o raritate – una de care nu dispuneam așa că m-am decis să călătoresc direct la Londra și să predau totul redacției de știri. Simțeam că aveam o poveste importantă despre niște soldați britanici foarte nemulțumiți, despre brutalitatea turcilor și despre compromiterea misiunilor NATO în partea de nord a Irakului. Aveam declarații din partea ofițerilor RAF și a piloților francezi care sprijineau ceea ce scrisesem.

Povestea a fost primită în tăcere. „Nu este chiar ce voiam de la tine”, a fost răspunsul. În cele din urmă mi s-a spus să rescriu tot și să vin cu un articol despre băieții noștri, nevoiți



să trăiască în corturi în deșerturile înghețate din Kurdistan, departe de casă și familie, tocmai când se apropia Crăciunul. De fapt, nu observasem prea multă nemulțumire în legătură cu corturile și condițiile de viață, cauza supărării tuturor erau satele bombardate cu napalm. Până la urmă, povestea n-a fost niciodată publicată. Oriunde aş fi dus-o, redactorii reacționau la fel – o primire rece și o ridicare din umeri: „Ne pare rău, nu-i pentru noi”. Nu înțelegeam de ce, fiindcă simțeam că e o problemă serioasă, care merita publicitate națională și internațională. N-a fost publicată niciodată, cel puțin nu în amănunt. La vremea respectivă am crezut că a fost din cauză că „Napalm și kurzi” era la polul opus al poveștii plăcute de Crăciun. M-am înșelat. Problemele dintre kurzi și turci erau prețul pe care trebuia să-l plătească alianța NATO și nu era în interesul nimănui ca problema să fie abordată în presă. Dezvăluirile ar fi putut pune în pericol disponibilitatea unor unități militare de mare valoare și compromite capacitatea NATO de a institui rezoluțiile Națiunilor Unite. Presa a acceptat să se conformeze și asta a fost tot.

De ce decide presa scrisă să omoare în fașă asemenea povești și să ignore un subiect care este evident de interes național? Există un anumit secret politic important, care n-a fost niciodată făcut public în Marea Britanie. El se leagă de sexualitatea unui politician laburist de vază, care deține în prezent o funcție importantă. Politicianul respectiv nu discută niciodată acest subiect și, totuși, fiecare redactor din Fleet Street îl cunoaște. În mod sigur va fi dezvăluit într-o bună zi și va avea repercusiuni semnificative, deoarece este un subiect pe care, în mod normal, ziarele de scandal l-ar înșfăca și l-ar storce până când și ultima picătură de potențial a fost extrasă. De asemenea, cititorii britanici vor vrea să știe (din interes public) de ce această poveste a fost ținută secret atâta timp. Când va exploda în sfârșit, politicianul respectiv va riposta într-o manieră demnă și reptilele vor începe să răstoarne pietrele până vor găsi ceea ce caută, dacă nu or avea deja acel lucru. Poate avea sau nu repercusiuni politice pe termen lung. E imposibil să-ți dai seama.

Întrebarea e: ce considerații conving presa să publice sau să respingă poveștile de acest fel? În cazul atrocităților comise de turci în Irak, se presupune că presa a fost convinsă că dezvăluirea acestor fapte n-ar fi în interesul țării și ar compromite anumite politici operaționale și strategice. E greu să susții această părere, astăzi, dar este posibil ca „muștruluiala turcilor” nu era nerecomandată de către guvern, și după câteva vorbe șoptite din partea unui ministru important, comunitatea din Fleet Street a decis să distrugă povestea. Cea de-a doua poveste a fost și ea suprimată, din cauza unei cereri venite direct de la părțile implicate. Nu e vorba de o problemă de conduită ilicită. Politicianul respectiv a cerut pur și simplu să se păstreze tăcerea și să nu fie făcute publice aspecte ale vieții lui private. Când subiecte importante nu devin știri și nu li se acordă atenție în presă, aceasta se datorează, de cele mai multe ori, înclinațiilor politice ale proprietarului și ale redactorilor săi executivi sau doar unei mici părți din rețeaua complexă de legături și promisiuni ce caracterizează relațiile din lumea știrilor. Proprietarii și redactorii lor discută împreună poveștile și se pun de acord să nu trădeze alți proprietari.

Alegerile generale din Marea Britanie au fost memorabile nu doar datorită aparentei limitări a direcțiilor politice puse în discuție, ci și datorită faptului că, pentru prima oară, partidele politice au organizat campanii electorale ultramoderne, controlate de echipe de manageri profesionale și foarte agresive. Partidul Laburist și Conservator au cheltuit împreună milioane de lire sterline pe transformări și campanii foarte avansate din punct de vedere tehnic, în încercarea de a influența cele opt sute de mii de alegători vitali din locurile marginale, care trebuiau convertiți la cauza partidului dacă voiau să câștige alegerile. Amândouă partidele știau că decizia finală urma să fie determinată de bătăliile locale aprige pentru acele locuri marginale și că acțiunea va avea loc departe de atenția mass-mediei. Ambele părți au făcut eforturi susținute pentru a identifica micile secțiuni de alegători necesare pentru a reuși. Liderii conservatori și laburiști au folosit cât mai mult

posibil elicopterele, pentru a se deplasa cu viteză în provincie în timpul campaniei electorale. A fost o goană nebună după voturi, atent planificată ca să se desfășoare rapid, și epuizantă din punct de vedere fizic. Michael Howard a afirmat că alegătorii care au contat pentru rezultatul final și care au trebuit convinși să renunțe la Noul Partid Laburist ca să existe speranțe pentru conservatori au fost în procentaj mai mic de 2%.

O mare parte din bugetul campaniei laburiștilor de 15 milioane de lire sterline a fost cheltuit în această bătălie pentru locurile marginale, purtată în circumscripțiile electorale vitale. Banii au fost alocați mai mult pentru goana după alegători decât pentru publicitate prin afișe și presă. Centrul Național Laburist de Comunicații din Newcastle a înregistrat două milioane și jumătate de apeluri telefonice către alegători în anul care a precedat anunțul alegerilor. Centrul național de apeluri al conservatorilor din Coleshill, lângă Coventry (Midlands), îi vâna, bineînțeles, pe aceiași alegători. La un moment dat, centrul de apeluri conservator trimitea zilnic un milion de fluturași și dădea un număr la fel de mare de telefoane. Convingerea prin telefon și poștă directă nu are prea mare valoare în alegerile politice dacă preocupările destinatarilor nu sunt înțelese și satisfăcute. Dacă unica preocupare a unui alegător o reprezintă țișanii care s-au mutat pe câmpul din spatele grădinii, nu prea are rost să i se vorbească despre pensii. Cei aproximativ un milion de alegători-țintă trebuiau studiați și convinși corespunzător prin scrisori sau apeluri telefonice, în care se explica politica partidului în legătură cu problemele care-i preocupau și în care era atacată politica partidului rival.

Ambele partide politice au folosit programe „cu captură de date” pentru a crea o bază de date din codurile poștale, fișele de bibliotecă și bazele de date ale cardurilor de fidelitate. Înaintea alegerilor, conservatorii au pus la punct sistemul Votervault, pentru a prezice probabilitatea ca un alegător individual să voteze cu ei sau împotriva lor. Au afirmat că programul avea o acuratețe de aproape 75%. Sursa săpăturilor

lor a rămas un mister, deși atât Experian, cât și Lexisnexis au fost implicate în consilierea partidului, și informațiile din cea mai mare bază de date națională de carduri de fidelitate au fost obținute prin companii de marketing cu date și folosite în monitorizare. Strategii asemănătoare pentru a ținti grupuri-cheie în statele sau districtele nehotărâte au fost folosite de campania Bush în alegerile din 2004.

Ambele partide au ținut mai puține conferințe de presă, iar Partidul Laburist în special a evitat ceea ce considera o presă în general ostilă și a preferat să caute contactul direct cu electoratul.

Singurul autocar electoral a fost folosit de vicepremierul John Prescott. Partidul Laburist, care a ținut înjur de trei sferturi de milion de alegători-cheie, a izolat cinci mii de votanți în toate cele 60 de circumscripții marginale-cheie. Le-au trimis tuturor prin poștă un DVD cu mesaje de la Tony Blair și de la candidatul laburist local, în care erau discutate subiecte locale. Acest exercițiu costisitor și ambițios a fost urmat de e-mailuri către o sută de alegători, în care li se spunea personal ce făcuse premierul în săptămâna respectivă, inclusiv faptul că fusese la Buckingham Palace să-i ceară reginei să dizolve Parlamentul, pentru a declanșa alegerile. Au mai făcut de asemenea un jurnal video zilnic, care apărea pe site-ul oficial al partidului, unde erau discutate din nou „punctele de maxim și minim interes” ale zilei și era repetat mesajul care spunea că va fi o campanie dură, în care se va lupta pentru fiecare loc. În tot acest timp, echipa condusă de Lyntori Crosby, geniul electoral australian, adus că să creeze și să se ocupe de campania conservatorilor, furniza presei liste cu ceea ce se pretindea a fi minciunile spuse de Blair publicului britanic.

Campania a fost memorabilă datorită afirmațiilor și contrazicerilor făcute în legătură cu cheltuielile. Acestea nu au fost doar transmise personal de către politicieni, ci au fost de asemenea dezvăluite presei prin „scurgeri” telefonice constante. Laburiștii au angajat o echipă de comunicații media pentru a trimite e-mailuri și a se concentra asupra jurnaliștilor

cu articole despre educație și sistemul național de sănătate. Materiale de acest gen sunt de obicei destinate scriitorilor de texte politice și grupurilor politice de „lobby” – grupul special de jurnaliști politici cu acces privilegiat la politicienii de marcă –, care rareori divulgă cine anume le-a furnizat informația. Dar pe măsură ce se desfășura campania, a devenit evident că ținta manevrării politice în timpul alegerilor nu mai era presa, ci deveniseră alegătorii-cheie marginali în persoană. Imboldul a venit din partea strategilor laburiști, zdruncinați de reacția publică negativă manifestată în timpul campaniei. Deși sondajele naționale arătau un avans al laburiștilor, partidul era îngrijorat, deoarece membrii importanți știau că adevărata campanie are loc departe de ochii presei în circumscripțiile marginale.

Unul dintre consilierii principali ai lui Blair a menționat un discurs ținut cu peste trei ani în urmă la Clubul Național de Presă din Australia. Vorbitorul era Lynton Crosby, care a condus Partidul Liberal al lui John Howard spre o victorie spectaculoasă în alegerile generale din Australia și care încerca acum să facă același lucru pentru Michael Howard. Crosby a atras atenția publicului său australian asupra faptului că, în ultimul timp, mulți comentatori din mass-media nu văd mare parte din campania adevărată. „Nu are loc la televizor, la radio și nici măcar în ziare. Activitatea locală pe teren e cea care contează cu adevărat – scrisori către alegători, cărți poștale, publicațiile de știri, propaganda prin telefon, bătutul la ușă...”

Politica s-a schimbat mult de la alegerile din 1997, când Partidul Laburist s-a bucurat de poziția sa neobișnuită de câștigător detașat într-o campanie unilaterală și a încurajat poveștile despre profesionalismul ingenios al organizatorilor campaniei, ca de exemplu al magicianului media Peter Mandelson și al secretarului de presă Alastair Campbell, un erou în domeniul relațiilor publice. Strategiile electorale adoptate de laburiști și conservatori în 2005 nu aduceau nimic nou. Cea care a deschis drumul tehnicilor de manipulare folosite de Howard și Blair a fost industria de marketing și PR.

Aceste tehnici au fost create pentru a cultiva influența ascunsă asupra presei în favoarea clienților lor din afaceri și partide politice favorabile afacerilor, ca „Noii Laburiști”. Colin Byfne, directorul gigantului de consultanță PR Weber Shandwick, fusese unul din principalii consultanți laburiști în probleme de manipulare. Ghidul Electoral Shandwick a atras atenția, încă înainte de a fi anunțată data alegerilor, că „în ciuda opiniei generale, campania din 2005 va face un efort concentrat pentru a ținti campania locală mai mult asupra locurilor-cheie marginale decât orice altă campanie media națională prezidențială”. A fost o schimbare revoluționară în politica electorală, care a fost îmbrățișată de ambele partide principale.

Din 2001, o mare parte a ideilor noi a fost importată din Statele Unite și, într-o măsură mai mică, din Australia: în special „marketingul prin permisiune”, folosit de mult timp în afaceri, a fost adoptat acum și de politică. „Marketingul prin permisiune” presupune folosirea sondajelor, a broșurilor și a scrisorilor pentru a-i încuraja pe alegători să răspundă direct unei campanii, să obțină, cu alte cuvinte, „permisiunea” alegătorilor individuali de a intra în dialog cu ei. Folosirea în acest fel a contactului direct permite angajaților partidului să vorbească despre subiectele de care este interesat în mod deosebit alegătorul individual. Acest sistem a fost folosit în campania electorală din 2005 de toate partidele politice importante. Conservatorii și laburiștii au investit din belșug într-un software care selecționează alegătorii în funcție de caracteristicile sociale, așa încât expedierile prin poștă și apelurile telefonice să poată fi adresate direct alegătorilor interesați în mod special de problema respectivă. În teorie, asta înseamnă că, de exemplu, proprietarii de case pot fi destinatarii mesajelor despre subiecte care îi privesc direct, ca ipotece și taxa de timbru. Votervault, așa cum a fost folosit de conservatori, a fost modelat după modelul american, în timp ce laburiștii au folosit Labour Contact, un pachet asemănător.

Nimic din toate acestea nu e vizibil pentru publicul larg sau presă. La începutul campaniei electorale, când site-ul

partidului a lansat un zvon despre posibilele campanii publicitare ale partidului, Alastair Campbell a fost văzut intrând în sediul Partidului Laburist, gata să se alăture campaniei. Una dintre temele următoare îl arătau pe Howard în pielea personajului Fagin al lui Charles Dickens, iar ziarele a luat-o razna condamnând antisemitismul imaginii. Rezultatul, după cum fusese bineînțeles prezis de Campbell, a fost că povestea a fost continuată la nesfârșit și le-a dat laburiștilor material din belșug. Partidul a publicat negări ample că ar fi avut motive ascunse, întărind în același timp afirmația că Partidul Conservator devenea zgârcit când era vorba de finanțarea sistemului național de sănătate. Scoaterea în evidență a originilor evreiești ale lui Howard și imaginea lui hipnotizând alegătorii cu un ceas de buzunar cu lanț s-a întipărit în minte. A fost o tactică abilă, deși nu putea fi folosită decât o singură dată. Conservatorii nu puteau pune punct poveștii, deoarece nu dețineau controlul asupra ei. Lui Howard i s-a cerut de sute de ori să comenteze, dar a refuzat.

Cele două partide principale și-au dezvoltat strategii în jurul „locurilor-cheie”, concentrându-și tot efortul asupra unui număr limitat de circumscriptii care ar fi putut schimba tabăra. Au reușit să dispună de baze naționale de telefonie, campanii naționale prin poștă, organizatori cu normă întreagă și vizite electorale din partea membrilor importanți de partid în aceste mici câmpuri de bătălie. În cazul laburiștilor, lista locurilor-cheie a ajuns la urechile presei și însuma 107 de circumscriptii electorale, toate deținute de laburiști în 2001. În cele din urmă, numărul a fost micșorat drastic în timpul celor patra săptămâni de campanie oficială. Propaganda din ușă în ușă și analiza ulterioară a reacțiilor și preocupărilor alegătorilor, folosirea grupurilor-eșalon și rapoartele regulate la sediu referitoare la mișcările celorlalte partide au fost introduse în baza de date a partidului și procesate.

Despre conservatori se știe că au avut o dezbatere internă la începutul campaniei, provocată de întrebarea dacă să aibă un număr limitat și „realist” de locuri-țintă sau o listă mai ambițioasă de obiective, întocmită pe baza câștigării

majorității. Liberal-democrații, care nu au reușit să concentreze resurse asemănătoare în campania lor, au fost totuși neîndurători cu selectarea alegătorilor-țintă și au încercat să urmeze o politică de „decapitare” a conservatorilor – concentrându-se, cu alte cuvinte, asupra membrilor importanți ai Partidului Conservator care dețineau așa-zisele locuri accesibile. Până la urmă, nu s-a dovedit o politică de succes. În cei doi ani care au precedat ziua alegerilor, principalele partide au efectuat sondaje de identificare a alegătorilor, campanii de propagandă cu broșuri și prin expediere directă în zonele de care erau interesați. Scopul propagandei electorale nu este neapărat schimbarea opiniei publice – ea este efectuată în așa fel încât agenții electorali să poată identifica potențialii susținători și să aprecieze atitudinea locală față de politica partidului. Partidele folosesc apoi propaganda și contactul direct, inclusiv până în ziua alegerilor, pentru a fi siguri că susținătorii cunoscuți vor merge să voteze. Alegătorii din circumscriptiile marginale sunt considerați neprețuiți, iar baza de date ale partidului este actualizată zilnic, pentru ca votanții să fie constant în atenție. O astfel de abordare n-ar funcționa niciodată dacă ai încerca să vinzi termopane în loc de filosofie politică.

Yotervault, Mozaic și Labour Contact sunt bunuri politice de mare preț și vor deveni tot mai importante, pe măsură ce vor crește în dimensiune. Informațiile, provenite din diverse surse, sunt introduse imediat ce sunt primite de la sediile celor două partide. În timpul alegerilor din 2005, informațiile le-au fost donate conservatorilor de către susținători ai partidului. Rezultatul alegerilor din 2005 a fost decis de propaganda electorală ascunsă și orientată spre piață. Una dintre controversele de durată legate de alegeri – în afară de bine-cunoscutul subiect referitor la Irak – a fost felul în care această campanie ascunsă urma să fie purtată, inclusiv intensificarea utilizării votului prin poștă și tehnicile folosite, care nu respectau recomandările Comisiei Electorale. Toate acestea au ridicat întrebări legate de manipulare și fraudă, ce vor trebui clarificate.



Conservatorii și-au asumat în mod sigur un risc în tehnicile lor de propagandă din 2005. Au folosit tacticile lui Crosby, precum „fluierul pentru câini” – adică marea masă a alegătorilor nu va „auzi” subiectele alese – ele putând fi ascultate și sprijinite de grupurile-țintă cărora li se adresează. În plus, au lansat atacuri la persoană mai răutăcioase decât orice alt mijloc folosit înainte. Deși partidul nu a reușit să ajungă din nou la putere, conservatorii au reintrat totuși în cursă ca un partid important după înfrângerile dezastruoase din precedentele două alegeri. Totuși, după standardele tradiționale ale „partidului de guvernământ”, a fost în mod clar o campanie murdară și incorectă. Lynton Crosby a fost aplaudat când a ținut un discurs lucrătorilor de la Biroul Central, cu două zile înaintea alegerilor. După încheierea numărătorii, se părea că tacticile lui îi aduseseră pe conservatori din nou pe linia de plutire. Mașinațiunile lui Crosby l-au zdruncinat pe Alastair Campbell, care a întocmit un dosar despre felul în care conservatorii au importat tactici dezonorante din Statele Unite și Australia. Într-o conferință de presă pentru jurnaliștii politici, s-a străduit să dea în vileag „trucurile murdare” ale conservatorilor, o sarcină dificilă pentru omul care întocmise mistificatorul dosar despre Irak. „Nimeni n-a mai încercat așa ceva în politica britanică”, a afirmat el.

Conservatorii au înțeles că, din punct de vedere tactic, nu se putea prezenta ca o alternativă la guvernare. În schimb, Crosby i-a modelat pe conservatori într-un vehicul, pentru a „trimite un mesaj lui Blair”. Strategia era: „Nu pierdeți timpul cu politici de partid, atacați opoziția”. La venirea lui, pe Crosby l-a îngrijorat lipsa arsenalului tactic al conservatorilor, așa că le-a spus că nu vor reuși să facă în șase luni ceea ce ar fi trebuit să facă în ultimii șase ani. A convins partidul să adopte „Strategia Queensland”, adică să transforme o poziție fără speranță într-un avantaj și să convingă alegătorii că „Nu veți câștiga, așa că votați cu conservatorii ca vot negativ, deoarece nu sunt o alternativă viabilă la guvernare”. Strategia funcționase în 1995 în Queensland, ținutul natal al lui Crosby,

dar în acest caz și-a asumat un risc considerabil, ținând cont că un astfel de stil negativ într-o campanie electorală ar putea convinge oamenii să nu mai voteze deloc.

Cealaltă tactică a sa, „fluierul pentru câini”, era o altă metodă pentru a „atrage rasiștii”. Enervați de succesul Partidului Independenței din Marea Britanie în alegerile din 2004 pentru Parlamentul European, conservatorii au decis să copieze mesajul acestuia împotriva imigrării, care presupunea o îndepărtare de Convenția de la Geneva în ceea ce-i privește pe refugiați, atrăgând astfel muncitorii – destinatarii acestui mesaj. Dar ar fi reușit ei să depășească numeric alegătorii burghezi de la oraș care ar fi putut să considere dezagreabilă orice aluzie la politica rasistă? Răspunsul depindea de felul în care s-ar fi achitat conservatorii în circumscripții ca Putney, pe care l-au și câștigat. În sfârșit, era bine să concentreze campania atât de mult pe Michael Howard? Howard fusese în trecut unul dintre cei mai antipatizați miniștri conservatori, iar schimbarea sa de imagine a fost remarcabilă. Dar nu era prea ușor de caricaturizat ca un vampir din întunecatul trecut conservator?

„Spargeți-i nasul lui Tony Blair”, a spus Brian Sedgemore, vechiul parlamentar laburist care și-a părăsit partidul în timpul campaniei electorale, din pricina opoziției sale față de Războiul din Irak. „Ștergeți-i rânjetul de pe față”, cereau manipulatorii conservatori. Alegătorii au făcut ambele lucruri, până la un punct, dar Blair a rămas la putere, deși n-a avut o expresie triumfătoare în discursul său de după victorie. A recunoscut că alegătorii au vrut să pedepsească guvernul. A menționat chiar și Războiul din Irak și a recunoscut că a dus la diviziuni, adăugând că speră că țara va fi unită din nou. Venind la sfârșitul unei campanii în care fusese caracterizat ca mincinos, un pericol pentru propriul partid, o pradă ușoară, și în care fusese păcălit de un jurnalist să discute despre viața sa sexuală, se ridică întrebarea: Poate Blair să revină? A promis să se retragă în timpul acestui mandat, lăsând puterea în mâinile ministrului de finanțe, Gordon Brown.

Sunt multe modalități de a interpreta aceste alegeri

derutante și meschine. Între 1979 și 1992, Partidul Laburist a pierdut patru alegeri la rând, și se părea că nu va fi niciodată ales. Până astăzi a reușit să contureze o nouă democrație socială britanică, în același timp, procentajul său de 36% din voturi populare este „cel mai mic de când Marea Britanie a devenit o democrație”, potrivit analistului politic Anthony King. În plus, nu este clar ce idei a lăsat în urmă Partidul Laburist. Promisiunea lui Blair din campania din 2001 de a face serviciile publice să răspundă cererii pieței, permițând oamenilor să-și aleagă singuri spitalele și școlile pe care le folosesc, a fost în mare parte amânată de concentrarea atenției asupra Irakului. De data aceasta, campania Noilor Laburiști semăna mai mult cu „vechiul” Partid Laburist, o promisiune nu de a face reforme, ci de a apăra serviciile de atacurile conservatorilor – „dacă țineți le asta, votați-ne”. Însă aceste trucuri murdare de analiză și marketing practicate de ambele părți sunt ceea ce va rămâne în memorie din alegerile electorale din 2005. Dar dacă ar dezvălui cineva toate informațiile secrete din dosarele ce se găsesc la Northcliff House? Ar fi ca și cum s-ar deschide cutia Pandorei...

## Concluzii

*Trăim vremuri periculoase. Suntem încă implicați într-un conflict major în Irak, unde un „război sfânt” între islam și America creștină continuă să facă victime, în Bagdad, infirmierele de la Centrul de Tratatament al Victimelor Torturii continuă să îngrijească irakieni ai căror tortionari nu mai sunt serviciile secrete ale lui Saddam, ci procurorii trimiși de CIA. Nu există încă o strategie de retragere a trupelor americane și britanice, iar președintele Bush încă zdrăngăne din spadă și amenință că va bombarda instalațiile nucleare din Iran. Cum s-a ajuns la asta? De ce au devenit liderii noștri atât de convinși că reprezintă forțele binelui în lupta cu un imperiu al răului? De ce vor să ne priveze de intimitatea noastră, să ne descopere cele mai ascunse secrete, să ne cunoască gândurile cele mai intime? Și de ce nu ne pasă suficient pentru a lua măsuri?*

Trăim într-o lume unde tot ceea ce spunem și facem poate fi înregistrat, monitorizat, așezat într-o bază de date, analizat, transmis serviciilor de securitate sau vândut unei companii specializate în marketing. Dacă urmăritorii noștri vor cu tot dinadinsul să vadă ce facem, ei pot îndrepta înspre noi un satelit de supraveghere, care ne poate detecta orice mișcare, zi sau noapte, în casă sau afară, pe furtună sau ceață. Ei pot, de asemenea, să se dispenseze de acest efort angajând o companie specializată în profiling. De la aceasta pot afla cine sunt vecinii noștri, ce sume avem în conturile noastre bancare, cât de mari sunt taxele pe care le plătim (sau nu le plătim), de unde ne cumpărăm medicamentele, numele și adresele iubitelor / iubiților, informațiile din cazier, inclusiv numărul de la pantof. Ei știu toate acele mici secrete murdare pe care ai vrea să le păstrezi departe de ochii autorităților.

Ceea ce trebuie să acceptăm acum este faptul că am renunțat la intimitatea noastră în urmă cu mulți ani. Nu am luat decizia conștientă de a ne abandona dreptul la viața privată fără ca alți oameni să-și bage nasul unde nu le fierbe oala, ci pur și simplu s-a întâmplat. Pur și simplu am făcut cu mâna, în semn de „bun-rămas”, tuturor măsurilor legislative pentru care au luptat înaintașii noștri, iar politicienii n-au avut habar ce se petrece. Nu am realizat că, în timp ce urmăritorii aflau tot ce voiau despre noi și transformau informațiile în profit, noi ne mulțumeam să ne uităm la televizor și să plecăm în vacanță. Așa că nu-mi pare deloc rău că am început ultimul capitol al acestei cărți reamintind cum Marea Britanie, până acum mai liberală și relaxată în comparație cu Statele Unite, s-a schimbat atât de mult.

Nu a durat mult pentru ca premierul britanic să fie copleșit de ceea ce el a numit „realitatea dură” și „bunul-simț” după 11 septembrie 2001. În 1994, Tony Blair, liderul opoziției la acea vreme, a spus în Camera Comunelor: „Un cetățean nu poate fi privat de libertate prin decizia unui politician, ci numai prin decizia unei instanțe judecătorești”. Cu toate acestea, ministrul de interne din guvernul lui Blair și-a acordat puteri excepționale, care îi permit să sechestreze la domiciliu orice persoană pe care o consideră o amenințare, fără ca decizia să treacă prin instanță. Reverendul Peter Selby, episcop de Worcester, a opinat, referindu-se la acest aspect: „Am rămas uimit când am văzut că guvernul a luat o măsură executivă într-un domeniu care îi aparține de drept puterii legislative”. Explicația este faptul că, atunci când țara este atacată de un inamic, la scară națională, publicul are tendința să creadă că politicienii percep situația ca pe o ocazie de a-și extinde puterile. Dificultatea este să-i convingi pe politicieni, când faptul este consumat, să renunțe la puterile extinse și să se reîntoarcă la vechiul sistem. Așa cum se poate întâmpla și cu libertățile cetățenești, cum sunt procesul cu jurați și prezumția de nevinovăție până la dovedirea vinovăției, dreptul nostru la viața privată numai înseamnă nimic acum.

Echelon, monstruosul sistem de colectare a datelor

sponsorizat de serviciile de securitate din Marea Britanie și Statele Unite și sprijinit de națiuni precum Canada și Australia, poate să recepționeze orice comunicație electronică între Orientul Mijlociu, Europa și Statele Unite, în orice moment al oricărei zile. Asta reprezintă o reușită tehnică remarcabilă, mai ales dacă te gândești că datele pe care le adună el sunt analizate, sortate, filtrate, rafinate electronic, până sunt reduse la materiale utilizabile, ce pot fi evaluate de niște ființe umane. Teoretic, doar datele ce se referă la criteriile stricte formulate de serviciile de securitate pot fi obținute astfel, dar cum putem ști asta cu siguranță? Programul Echelon este revoluționar și nu a fost copiat nicăieri, în primul rând deoarece Statele Unite au resursele umane și tehnice cerute, precum sateliți militari de supraveghere foarte sofisticăți și stații de monitorizare la sol cu personal calificat. Totuși, francezii au acum propriul sistem – desigur, mai mic, dar, la fel ca Echelon, cu baza în spațiu. Acesta este începutul unei curse. Când a început totul?

La o lună după atacul asupra World Trade Center („turnurile gemene”), administrația Bush a adoptat, Actul Patriotic” și, în acest proces, a inițiat atacul aferent asupra libertăților cetățenești. Președintele Bush și susținătorii săi își percep națiunea ca pe „Fortăreața America”, angajată într-un global „război împotriva terorii”, iar asta le oferă justificarea de care au nevoie pentru a ataca Afghanistanul și a mărșălui apoi prin Irak. Guvernul britanic, utilizând mulțimi de trafic de informații din întreaga lume, a strâns suspiecții de terorism și i-a închis într-un gulag de închisori de înaltă securitate. Când, într-un final, sistemul judiciar a spus guvernului că încalcă principiile constituționale, toți suspiecții au fost eliberați, înainte de a schimba Constituția pentru a le permite să aresteze la domiciliu pe oricine ar vrea, fără punere sub acuzație și proces.

Actualele dispute dintre partide în privința Constituției din Marea Britanie trebuie asociate cu atacurile prelungite asupra libertăților cetățenești. Acestea includ nu doar un atac asupra principiilor procesului cu jurați și asupra prezumției de

nevinovăție, dar și cererea ca fiecare să-și dovedească existența plătind pentru propriul card de identitate. Toate acestea reprezintă tentative grave de a înclina balanța puterii constituționale în favoarea executivului. Sunt cereri care, chiar și în Statele Unite, ar fi respinse imediat de Senat. Guvernul britanic a profitat de oportunitatea oferită de o majoritate parlamentară masivă pentru a corupe administrația, chiar luând puterea din mâinile funcționarilor de stat și dându-le-o unor „aparatnici” sau „consilieri” nealeși și pornind la război în Irak, pe baza unor sfaturi neoficiale și îndoielnice venite de la Procurorul General. Guvernul a ieșit basma curată după toate aceste abuzuri grație majorității sale parlamentare, satisfacției oferite de o economie aparent sănătoasă, precum și faptului că membrii electoratului destul de furioși pentru a răsturna situația sunt prea puțini.

Cea mai semnificativă pierdere a libertății, care a trecut aproape neobservată de public, este nivelul de siguranță dăunător și constant care s-a strecurat în viața cotidiană a tuturor britanicilor. Electoratul observă foarte greu acest lucru, deoarece votanții sunt mai preocupați de taxe și impozite, guvernare locală și centrală, imigrație și legislație. Însă va veni o zi când ei vor realiza că libertatea lor, odinioară cel mai valoros premiu, a dispărut pentru totdeauna.

Pierderea intimității nu a fost determinată doar de deciziile politicianilor, ea a rezultat și din activități comerciale. E limpede că în prezent există o uriașă piață internațională a informațiilor, în care datele pot fi vândute sau schimbate cu parteneri din întreaga lume, în pofida asigurărilor enunțate în Legea protecției datelor și în Legea libertății informațiilor. În lumea „rețelei”, companiile de marketing cu date trebuie să fie active în arena internațională pentru a putea spera la succesul financiar. Marii jucători, care concurează unii împotriva celorlalți și folosesc poveștile noastre de viață ca materiale brute, sunt prea bogați și puternici pentru ca politicienii piperniciți să se opună eficient în mod legislativ.

Piața informațiilor va înflori pentru că bazele de date sunt pretutindeni. Cea a Serviciului Național de Sănătate (NHS)

conține înregistrările medicale ale tuturor persoanelor din Marea Britanie. Pare trist că această conversie a tuturor datelor în formă computerizată anunță sfârșitul acelor caiete-index vechi, conținând notițele medicilor de familie cu scrisul lor, prin tradiție indescifrabil. Acele caiete cu mângălituri străvechi, pete de cafea și hieroglife bizare, formule chimice complicate, detalii intime ale vieții sexuale familiale, ale bolilor, accidentelor dureroase și ale disfuncțiilor jenante genito-urinare au fost toate traduse cumva în limbajul computerelor. Eufemismele doctorilor, deseori scrise codat (de pildă „MDB” pentru „mort de beat”) cu stiloul, pixul cu mină sau uneori creionul, au devenit desuete, acum că au fost transcrise într-o bază de date uriașă, care va fi deschisă membrilor „acreditați” ai Serviciului Național de Sănătate.

De fapt, potențialul de a se strecura erori va fi foarte mare și, în consecință, riscul asupra sănătății – grav. Asta e ceea ce guvernul descrie drept „progres”, dar cea mai îngrijorătoare este pierderea controlului asupra acestei neprețuite resurse private. Simpla sa existență face ca personalul spitalului în care ești primit pentru a te opera de prostată sau pentru a-ți extrage măselele de minte va putea avea acces la istoria ta privată. Ca o consecință directă a creșterii industriei de colectare a datelor, câțiva dintre cei privilegiați, care au acces la asemenea date confidențiale, vor primi stimulente serioase pentru a le vinde celor care pot profita cel mai mult de pe urma lor. Aici sunt incluși nenumărați funcționari guvernamentali, administratori sanitari, consultanți, asistente, generaliști și paramedici, care vor dispune de acces facil la detaliile tale personale, chiar dacă asta este împotriva codului lor de bune practici.

Sănătatea va fi urmată curând și de educație. Înregistrările școlare de la autoritățile locale de sănătate vor fi adnotate și transferate într-o bază de date a Departamentului pentru Educație. Ce va include ea? Prezența la școală, pedepsele aplicate de profesori, notele pentru teme și rezultatele testelor? Opinii particulare ale unor dascăli ostili sau ale unor inspectori școlari? Vor fi aceste informații disponibile unor



angajatori potențiali, care vor putea fi tentați să își bazeze judecățile pe opiniile profesorilor privind caracterul aplicantului, exprimate pe când acesta avea 12 ani? Cu toții ne schimbăm cu timpul. Ne maturizăm și ne dezvoltăm fizic, mental și emoțional. Creșterea și dezvoltarea sunt, desigur, influențate de experiențele trăite. Datele, așa cum reies din computer, sunt la fel de aride ca un schelet în deșert. Ele se bazează pe analize, deseori purtate automat de programul computerului, pentru a pune came pe oasele goale. Este un fapt foarte îngrijorător că, în această formă brută, cantități imense de date sunt colectate fără permisiunea noastră sau fără vreo asigurare reală că ele nu vor cădea în mâinile unor persoane nepotrivite.

Nimic nu este mai adevărat decât maxima: „Informația înseamnă putere” și e evident că toți politicienii o acceptă fără a pune întrebări. Totuși, nu există o legislație relevantă care să ne protejeze împotriva utilizării nepotrivite a detaliilor noastre private. Legea protecției datelor nu face prea multe pentru a împiedica executivul să strângă și să păstreze informații despre viețile noastre. Oare protecția nu ar trebui să preceadă colectarea?

Îndoiala supărătoare pe care nu mi-o pot scoate din minte este: cât de sigure vor fi înregistrările mele de sănătate și educație? Acest lucru e important pentru mine, deoarece nu vreau ca vreun broker de asigurări să afle că am avut febră reumatică în copilărie (ceea ce nu e adevărat) sau că am fost dat afară din școală pentru consum de droguri la 15 ani (ceea ce nu s-a întâmplat) sau că am avut o programare la clinica de boli venerice din Praed Street după ce am descoperit un furuncul urât la 18 ani (ceea ce poate fi adevărat). Însă mai rău decât potențială pierdere a intimității și confidențialității este înțelegerea faptului că baza de date a NHS-ului va fi una dintre cele mai complexe tentative din istorie de colectare a informațiilor. Confidențialitatea ei este vitală pentru toți britanicii care pun preț pe sanctitatea vieții lor private. Totuși, este responsabilitatea politicienilor și a funcționarilor publici să se asigure că nicio înregistrare medicală nu va cădea pe

măinile cui nu trebuie. Este o însărcinare fără speranță de reușită. Vor apărea tot felul de măsuri legislative și promisiuni de pedepse grele pentru cei prinși exploatând datele, însă industriile medicamentelor și asigurărilor sunt multinaționale, iar valoarea înregistrărilor medicale ale unei națiuni este inestimabilă.

Același lucru este valabil și în cazul educației. De ce ar trebui ca opiniile personale și foarte subiective din urmă cu ani buni ale unor persoane să fie accesibile azi fără permisiunea subiectului acestor afirmații? Mă tem că vor trece nu ani, ci luni până când poveștile vieților unui uriaș număr de cetățeni britanici să ajungă pe mâna companiilor farmaceutice și nu numai, care le pot achiziționa. Când se va întâmpla acest lucru, mass-media, mereu nerăbdătoare să afle lucruri explicite și personale despre public, își va pierde orice inhibiție pe care ar putea-o avea privind întrebuintarea abuzivă a datelor personale, dacă asta înseamnă că ar putea pune mâna pe detaliile privind dezintoxicarea sau comportamentul sexual din școală al vreunui star rock.

Bazele de date sunt produse ale tuturor departamentelor guvernamentale. Odată ce informațiile de pe cardul de identitate sunt puse în comun și verificate prin comparație cu alte date personale, incluzându-le pe cele de la Administrația Financiară sau de la Departamentul Vamă și Accize, cazierul și baza de date tot mai mare a poliției, incluzând informații pentru recunoașterea facială, baza de date a NHS-ului, uriașa cantitate de cunoștințe obținute și păstrate de pe smart carduri și carduri de credit, înregistrările serviciului de Imigrație, baza de date a Departamentului pentru Educație, Biroul Pașapoarte, permisele de conducere, conturile bancare și de la biblioteci, Registrul Național de Nașteri, Căsătorii și Decese – totul despre noi va fi știut. Asta e probabil mai mult decât știm despre noi înșine.

Dacă publicul nu se va revolta împotriva întrebuintării abuzive a informațiilor care există deja în Marea Britanie și în Statele Unite, baze de date enorme precum aceasta vor exista în mai puțin de 20 de ani. Banalul card de identitate va fi

înlocuit cu o poveste a vieții fiecăruia dintre noi, deținută de stat. Datele vor fi inexacte, iar existența lor – profund neliberală. Totuși, dosarele noastre cibernetice vor fi folosite pentru ca alții să-și formeze păreri despre noi și ar putea deveni bazele unui stat polițienesc. Statele Unite ne-au deschis drumul cu programul CAPPSN, menit a alcătui profilul întregii populații, pentru a identifica potențialii teroriști pe listele de zbor ale avioanelor. Când știi tot ce se poate ști despre o populație, iar informațiile sunt conservate electronic, poți începe să tragi concluzii pe baza tuturor cunoștințelor acumulate. Referințele încrucișate și profilurile personale sunt deja practici comune. Nu e greu să ne imaginăm ce consecințe groaznice ne așteaptă dacă tehnologia aceasta va ajunge în mâinile unui stat foarte represiv.

Colectarea de date va continua și serviciile de spionaj vor deveni tot mai puternice, adăugând sos la puternicul amestec de informații obținute din înregistrări publice. MI5 și MI6, cele două brațe ale serviciilor secrete britanice, sunt însărcinate cu spionajul național, respectiv internațional. Ambele servicii au cunoscut cel mai înalt nivel de alertă – „severă” (generală) – din noiembrie 2003, când Al Qaeda a bombardat clădirea Consulatului Britanic din Istanbul, ucigându-i pe consulul general și alte 25 de persoane. „Alertă severă” înseamnă că un atac terorist este așteptat și pe sol britanic și toate unitățile antiteroriste ale poliției, serviciilor secrete și armatei, precum și serviciile de urgență trebuie să fie mereu pregătite. MI5, serviciul de securitate internă, își are baza la patru sute de metri mai sus de Parlament pe Tamisa, la Thames House, lângă Galeriile Tate. Directorul General, Eliza Manningham-Buller, o spioană arțăgoasă și carieristă, a fost nevoită să-și asume vina pentru eșecurile spionajului la începuturile Războiului din Irak. Atât MI5, cât și MI6 au fost supuse unor reforme impetuoase de când premierul Tony Blair a luat decizia de a intra în război, la 45 de minute după ce s-a afirmat că arme de distrugere în masă ar putea fi îndreptate asupra țării. Serviciile de securitate au mai fost acuzate că l-au identificat pe doctorul David Kelly, expertul în arme chimice

care și-a luat viața când oamenii au fost scandalizați că dosarul care se presupunea că dă detalii despre resursele militare ale lui Saddam fusese de fapt falsificat. Era clar că trebuia făcut ceva după ce raportul Lordului Butler a afirmat că MI6 s-a înșelat privind armele deținute de Saddam Hussein.

Reforma serviciilor de spionaj britanice a venit ca un anunț tipic vag, ce înșira noi standarde de raportare și verificare a erorilor, numirea unui nou șef al Analizei Informațiilor care să supravegheze activitatea spionilor și o „Cartă Whistleblower” care le permite analiștilor îngrijorați că datele sunt contrafăcute să-și dezvăluie îndoielile, fără să se teamă de repercusiuni ce le-ar putea periclita cariera. Agenția a mai recrutat un „Consilier al personalului”, care va sta la dispoziția analiștilor și oficialilor nemulțumiți de modul în care este folosit materialul. Mai mulți analiști au fost recrutați în MI6 și au fost adoptați „termeni-standard” pentru a descrie gradul de încredere al surselor secrete. Totuși, guvernul britanic a acceptat că dosarul pregătit ca parte a justificării de a intra în război cu Irakul era eronat și că viitoarele rapoarte precum acesta ar trebui să separe clar opiniile ministeriale de aserțiunile Comitetului Unit de Informații.

Pare ciudat faptul că spionii noștri sunt monitorizați și îndrumați cu atâta atenție, iar comportamentul lor este analizat la sânge de stat, câtă vreme politicienii care au dat declarațiile privind amenințarea cu arme chimice de 45 de minute rămân mai presus de orice critică. În timp ce ministrul de la externe anunța reformele aduse serviciilor de spionaj și cum vor trebui ele să raporteze informațiile secrete de acum înainte, MI5, care are câteva sute de ofițeri implicați permanent în activități antiteroriste, recruta în Marea Britanie 1.000 de noi angajați. A mai fost stabilită o rețea de „birouri” locale, care să țină sub observație amenințările regionale. Numărul persoanelor implicate în spionarea britanicilor crește constant și, în timp ce activitățile lor sunt, desigur, ținute secrete, spionii au devenit mai vizibili și mai puternici în ultimii ani. În Londra, SOI3, grupul antiterorist al poliției, angajează 900 de ofițeri pentru Divizia Specială (S012) și

Divizia Antitero (S013), iar alți 1.500 au fost desfășurați în forțele regionale din West Mainlands, Manchester și Scoția. Unitatea de supraveghere de elită a armatei, Compania 14 de Spionaj, care s-a ocupat mulți ani de monitorizarea celulelor teroriste republicane și loialiste din Irlanda de Nord, a fost mutată pentru a sprijini regimentele militare specializate, precum SAS și ZBE, în viitoarele lor operații din afara Marii Britanii. Unitatea e acum cunoscută ca Regimentul Special de Recunoaștere și staționează la Hereford (alături de SAS). Sarcina regimentului este de a oferi servicii de supraveghere secretă asupra organizațiilor teroriste înainte de intervenția forțelor speciale. Este unul dintre cele mai respectate regimente ale forțelor armate britanice, iar probabila sa deplasare în Irak vine ca urmare a solicitării armatei americane. Deși e o unitate mică, având mai puțin de 100 de bărbați și femei, experiența lor în supraveghere, căpătată pe străzile însângerate ale Belfastului, este considerată unică.

Creșterea numărului de cadre utilizate în activități de spionaj și informații secrete pe teritoriul continental britanic s-a produs în mod evident ca răspuns la ceea ce se percepea a fi o amenințare reală. Dar Eliza Manningham-Buller omite să spună cât de mare este această amenințare. În particular, ea refuză să ofere cifre pentru că e de părere că, pe lângă un grup mic de teroriști devotați cauzei lor, pe teritoriul continental există un număr nedefinit de simpatizanți care ar putea sau nu să ofere sprijin, dar care s-ar face că nu știu nimic despre activitățile teroriste ale celorlalți dacă ar fi întrebați. O sursă neoficială MI5 a estimat că până la 3.000 de tineri musulmani britanici au participat la taberele de antrenament ale Al Qaeda înainte ca acestea să fie închise în 2002. Lordul Hoffinan, responsabilul juridic care a inspectat suspiecții deținuți fără proces la Belmarsh, crede că cifra se apropie de 1.000.

Ocazional, apar diverse informații oferite de serviciile secrete, cum ar fi faptul că Centrul Unit de Analiză a Terorismului de la Thames House a primit 60.000 de informații despre un atac iminent și că atacul, când și dacă se

va întâmpla, va fi un atac convențional sinucigaș cu bombă în timpul unui moment important, cum ar fi alegerile generale sau începutul unei noi sesiunii a Parlamentului. Dar stă în firea Al Qaeda să lovească în momente neașteptate ținte neprevăzute. Osama Bin Laden este un strateg strălucit, iar timpul este în mâinile sale. La un summit internațional despre „Democrație, terorism și securitate”, ținut la Madrid în 2005, s-a insistat asupra ideii că este vital să se lupte împotriva terorismului fără a compromite libertatea. Una dintre concluzii era că agențiile care aplică legea au nevoie de puteri pentru a-și face treaba, dar că nu trebuie să sacrifice niciodată principiile pe care sunt menite să le apere.

Problema este că serviciile secrete nu au acceptat niciodată că trebuie să joace un rol în procesul juridic și multe din lucrurile pe care le fac rămân neînregistrate. După părerea agentului secret profesionist, suspiciunea este suficientă pentru a închide pe cineva. Serviciile secrete sunt întotdeauna refractare la oferirea de „probe” dacă în felul acesta le e compromisă sursa. Activitățile lor nu trebuie expuse niciodată analizei și examinării minuțioase a vreunui tribunal regal, spun ei. Interceptarea apelurilor telefonice a fost ilegală în Marea Britanie până la mijlocul anilor 1980. Puteai să faci înregistrări dacă făceai o cerere la Ministerul de Interne și ți se aproba. Pentru a putea fi efectuată, interceptarea trebuia să facă parte dintr-o investigație privind activități criminale deosebite sau să aibă de a face cu apărarea securității statului, și asta numai dacă informația nu putea fi obținută în alt mod. Dar apoi legislația s-a relaxat. Imediat au apărut povești despre comportamentul incorect al agenților MI5, care, pe lângă spionarea ambasadelor și consulatelor țărilor de dincolo de Cortina de Fier, au început să se amestece și în treburile sindicatelor și organizațiilor cum ar Campania pentru Dezarmare Nucleară (CDN). Aceasta nu a avut nimic de a face cu un proces legal. MI5 nu a încercat să construiască un caz legal, ci doar aduna informații secrete și construia o imagine pentru a arăta că „știa ce se întâmplă”. Nu a existat nici cea mai vagă sugestie că vreuna dintre conversațiile înregistrate

de MI5 va fi folosită în vreun proces.

O hotărâre a Curții Europene a Drepturilor Omului a obligat guvernul să promulge în 1985 Legea interceptării comunicațiilor, care stabilea condițiile generale de desfășurare a interceptărilor. Actul păcătuia însă prin aceea că excludea total tribunalele din această chestiune. Printre altele, legea stabilea ca pe durata procesului să fie interzise prezentarea dovezilor sau întrebările care ar fi putut indica existența unei interceptări, fie aceasta cu sau fără mandat. Pasajul în cauză a fost introdus deoarece serviciile secrete se temeau că în timpul proceselor s-ar fi putut face referire la activitățile lor ilegale de interceptare a convorbirilor din trecut, care între timp deveniseră legale, și că ar putea trage ponoasele de pe urma ilegalităților pe care le comiteau încă. Nici măcar în cazurile de siguranță națională nu sunt permise dovezile provenite din interceptări. Reprezentanții sistemului judiciar resping aceste măsuri speciale, în primul rând deoarece astfel ofițerii și spionii serviciilor secrete primesc imunitate în fața justiției. Judecătorii nu privesc cu ochi buni nici faptul că guvernul a susținut această decizie. Poliția, procuratura, grupul de presiune Liberty, Comitetul parlamentar reunit al drepturilor omului, toate aceste organisme au catalogat restricțiile ca fiind „ridicole”. George Churchill-Coleman, fost șef al unității antiteroriste a Scotland Yard, a atras atenția asupra faptului că Marea Britanie devine din ce în ce mult un stat polițienesc: „Refuzul serviciilor secrete de a consimți ca dovezile obținute din interceptări să poată fi utilizate în sălile de judecată, precum și ajutorul de care s-au bucurat din partea stăpânilor lor politici sunt dovezi străvezii ale faptului că este dorința comună a unor factori de decizie importanți din sistemul nostru politic și de siguranță națională să devenim în scurt timp un stat polițienesc”.

Serviciile secrete britanice răspund doar în fața unui atotputernic director, care a dovedit de nenumărate ori că nu are scrupule în a scormoni în viețile noastre pentru a-și atinge propriile scopuri. Pe măsură ce MI5 și MI6, precum și bazele de date naționale se dezvoltă, scenariile apocaliptice privind

atentate teroriste viitoare se vor înmulți, până când, în ciuda puținătății dovezilor, teama pentru propria noastră siguranță va învinge nevoia de intimitate. Militarii în rezervă rareori văd într-un card de identitate un atentat la drepturile civile, deoarece au purtat un card de acces de-a lungul întregii lor cariere.

Mulți civili, de toate condițiile și cu pregătiri din cele mai diferite, nu consideră că au de ce să se teamă de o bucată dreptunghiulară de plastic. Desigur, nu cardul de identitate în sine pune în pericol drepturile cetățenești, ci proliferarea camerelor de supraveghere și a bazelor de date internaționale, coroborate cu activitatea acerbă și în forță a poliției și a serviciilor secrete, care se bucură în prezent de toate resursele de care ar putea avea nevoie în lupta cu terorismul. Luați în calcul de asemenea voința politică pentru ca nimeni din Marea Britanie și America să nu fie lăsat în plata Domnului, precum și viteza amețitoare cu care se dezvoltă noile tehnologii, și veți recunoaște semnele rău-prevestitoare.

Centrala de interceptare americană de la Menwith Hill și complexul destinat spionajului electronic de la GCHQ din Cheltenham, Marea Britanie, pot monitoriza toate telefoanele și e-mailurile transmise din sau tranzitând arhipelagul britanic. Și, dacă o pot face, fiți siguri că nu o să se gândească de două ori. Desigur, personalul este insuficient pentru a monitoriza absolut toate comunicațiile; oricum, cea mai mare parte dintre acestea nu valorează nimic pentru părțile interesate, fie că vorbim de fisc, de poliție sau de lanțul de retail Tesco. Prin intermediul unui soft se pot selecta, însă, materialele relevante; cuvinte și fraze-cheie, surse și destinații suspecte, limbi străine folosite, toate pot fi identificate și aduse în atenția serviciilor secrete. Programele și viteza de calcul sunt îmbunătățite constant, deoarece nevoia de informații crește de la o zi la alta.

Conștientă de fluxul de populație din Europa și Orientul Apropiat, CIA se folosește permanent de resursele impresionante de calcul de care dispune pentru a analiza și a aduce la zi lista persoanelor considerate ca fiind „suspecte”.



Această bază de date conține 6.000 de nume și se alcătuieste prin coroborarea mai multor criterii, cum ar fi tipare de mișcare (destinațiile de călătorie și frecvența vizitelor), locul nașterii, ba chiar numele și adresele rudelor. Această listă de nume este împărtășită cu state partenere. Monitorizarea se realizează în Statele Unite, în Marea Britanie și în Europa continentală, iar serviciile secrete britanice sunt îmboldite permanent să furnizeze agențiilor americane orice aspect semnificativ privind activitatea persoanelor de pe listă.

George Friedman, fondator al reputei Stratfor, agenție independentă de informații cu sediul în Statele Unite, consideră că problema serviciilor secrete britanice și americane este tendința lor de a se bizui pe „surse și informații, mai degrabă decât pe o cunoaștere reală, din interior, a problemelor”. Sursele secrete și bazele de date pot fi utilizate pentru a susține o analiză; nu și o idee, însă. Nimeni nu poate lua o hotărâre fără să se bazeze pe informațiile furnizate de surse sau de baze de date. Când cineva o face și dă greș, atunci e vai de pielea lui. CIA și MI5 sunt cum nu se poate mai minuțioase în chestiunile de mică importanță, dar au tendința să se înșele cu totul în ceea ce privește problemele importante. Sediul CIA din Langley, Virginia, geme de ofițeri care susțin că au prezis atacul asupra turnurilor gemene de la 11 septembrie. Ce-i drept, anterior atentatului, au avut loc exerciții în care teroriști arabi intrau cu avioane de linie în World Trade Center. Era doar unul dintre sutele de scenarii posibile și nu a fost luat în serios. Teoria CIA conform căreia Al Qaeda era răspândită la nivel global și avea drept țintă Statele Unite se baza pe viziune, nu pe dovezi ori pe informații strânse de la surse. Când agenții CIA au aflat de la surse că agenții Al Qaeda aveau bază într-un oraș european, această informație a fost introdusă într-o analiză. Câteva zile după 9/11, CIA nu avea nici cea mai mică idee dacă Statele Unite se aflau în război cu Vestul sau aveau de-a face cu o șleahță de infractori.

Viziunea apare rar în serviciile secrete; când apare, la Langley nu e bine-venită și la Thames House e hulită de-a

dreptul. Rezultatul e cel enunțat anterior: CIA și MI6 se pricep la nimicuri, dar le lipsește imaginea de ansamblu. Ofițerii și conducerea se bazează doar pe informațiile și analizele obținute de la surse umane și pe aportul bazelor de date secrete pentru a-și întemeia hotărârile, conștiință permanent de ceea ce stăpânii lor din sfera politicului ar dori să citească în informările pe care le primesc, venind permanent în întâmpinarea dorințelor lor.

Următorii zece ani vor fi caracterizați fie de o sporire exponențială a cantității de informații personale strânse de către stat, fie de o revoltă spontană împotriva încălcării dreptului la viața privată. Combatanții acestei lupte vor fi, pe de-o parte, publicul și organizațiile nonguvernamentale, și politicienii și marile corporații, care văd în oameni niște instrumente de marketing, bune doar să muncească și să voteze, de cealaltă parte. Nu există interes public pe care această ultimă perspectivă să-l servească. Nu există onoare în acest punct de vedere. Mama mea, văduvă la peste 90 de ani, trăia într-un azil de bătrâni și, totuși, primea regulat scrisori de la marile trusturi financiare. Nu o deranja, deoarece simțea că astfel stabilește o punte de comunicare cu lumea exterioară. Nimeni nu le cerea, și totuși scrisorile continuau să vină, cu scopul vădit de a profita de pe urma vulnerabilității ei. Mai vorbeam din când în când cu ea, pentru a-i lua apoi scrisorile și a le arde. În cele din urmă, corespondența nesolicitată a fost interzisă la azilul unde era mama internată când un bătrân și-a pierdut averea după ce a răspuns la o astfel de scrisoare. Informația înseamnă putere, dar impune responsabilitate. Avem nevoie de o legislație adecvată pentru a ne asigura de utilizarea înțeleaptă a informației, pentru a preveni exploatarea celor vulnerabili.

De ce nu am face ceva ACUM pentru a opri această încălcare a drepturilor noastre civile? Se impune revizuirea de urgență a legii privind viața privată. Când dezbaterea privind cardul de identitate va reveni în Parlament, s-ar putea să fie ultima noastră șansă să scăpăm de pacostea asta, o dată pentru totdeauna.

Și, dacă tot ne vom fi apucat, am putea băga și guvernul, și corporațiile în curățenie generală, mai cu seamă colțurile murdare unde sunt strânse secretele noastre pentru a fi introduse în computere, acelea în care se pregătește folosirea lor împotriva noastră. Un prim pas ar putea fi desființarea monopolurilor de stat și comerciale de colectare a informațiilor despre alegători, aflate deocamdată în afara oricărui control. Avem nevoie, mai ales, de o legislație nouă, care să instituie dreptul nostru la viața privată, care să ne lase să ne trăim viața, fără imixtiunea statului și a marilor companii. Abia atunci libertățile despre care credeam că ni se cuvin de la naștere, dar de care suntem privați încet-încet, vor fi instaurate o dată pentru totdeauna.

## Bibliografie

Ball, Kristee S. și Webster, Frank, *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, Pluto Press Ltd, 2003

Berkowh, Bruce D. și Goodman, Allen E., *Best Truth: Intelligence in the Information Age*, Yale University Press, 2002

Brin, David G., *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Perseus Books, 1999

Corbin, Jane, *The Base: Al Qaeda and the Changing Face of Global Terror*, Pocket Books, 2003

Deamley, James și John Feather, *The Wired World: An Introduction to the Theory and Practice of the Information Society*, Library Association, 2001

Denning, Dorothy E., *Information Warfare and Security*, Addison Wesley, 1999

Drakos, Peter și John Braithwaite, *Information Feudalism: Who Cums the Knowledge Economy*, Earthscan Publications, 2002

Feather, John, *The Information Society: A Study of Continuity and Change*, Facet Publishing, 2004

Frank, Mitch, *Understanding September 11th: Answering Questions about the Attack on America* „Viking Books, 2002

Garhinkel, Simpson, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly UK, 2001

Garland, David, *The Culture of Control: Crime and Social Order în Contemporary Society*, Oxford University Press, 2002

Lessig, Lawrence, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, Penguin USA, 2004

Levin, Thomas Y., *CTRL (Space): Rhetorics of Surveillance from Bentham to Big Brother*, MIT Press, 2002

Lyon, David, *Surveillance after September 11*, Blackwell Publishing, 2003

Lyon, David, *Surveillance as Social Sorting: Privacy, Risk, and*

*Automated Discrimination*, Routledge, 2002 Lyon, David, *Surveillance Society: Monitoring Everyday Life*, Open University Press, 2001

Mackey, Chris și Greg Miller, *The Interrogator's War: Inside the Secret War Against Al Qaeda*, John Murray, 2004 Mcgrath, John, *Loving Big Brother: Surveillance Culture and Performance Space*, Routledge, 2004 O'Harrow, Robert, *No Place to Hide*, Free Press, 2005 Parker, John, *Total Surveillance: Investigating the Big Brother World of E-spies, Evesdroppers and CCTV*, Piatkus, 2001 Rai, Milan, *Regime Unchanged: Why the War în Iraq Changed Nothing*, Pluto Press, 2003

Ramesh, Randeep, *The War We Could Not Stop: The Real Story of the Battle for Iraq*, Faber and Faber, 2003 Riddell, Peter, *Hug Them Close: Blair, Clinton, Bush and the "Special Relationship"*, Politicos, 2004.

Riddell, Peter, *The Hidden Hand: Britain, America and Cold War Secret Intelligence*, John Murray, 2002 Ritter, Scott, *WaronIraq: What Te-am Bush Doesn't Want You to Know*, Profile Books, 2002

Schulsky, Abram M. și Gary J. Schmitt (ed. Gary J. Schmitt), *Silent Warfare: Understanding the World of Intelligence*, Brassey's US, 2002

Sefry, Micah L. și Christopher Cerf (eds.), *The Iraq War Reader: History, Documents, Opinions*, Touchstone Books, 2003 Silvers, Robert B. și Barbara Epstein, *Striking Terror: America's New War*, New York Review of Books, 2002 Simpson, John, *The Wars Against Saddam: Taking the Hard Road to Baghdad*, Macmillan, 2003

Stauber, John, *Weapons of Mass Deception*, Constable and Robinson, 2003

Stothard, Peter, *30 Days: A Month at the Heart of Blair's War*, Harpercollins, 2003

Todd, Paul și Jonathan Bloch, *Global Intelligence: The World's Secret Services Today*, Zed Books, 2003 Webster, Frank, *Theories of the Information Society*, Routledge, 2002 Webster, Frank și Ensio Puoskari, *The Information Society Reader*, Routledge, 2003

Woodward, *Plan of Attack*, Simon and Schuster, 2004